كفاءة احترام البيانات الشخصية

L’efficience du respect des données personnelles

إعداد: السعيدي بشرى

دكتوراه في القانون الخاص، القانون الجنائي البيئي، المغرب

تاريخ الاستلام: 2024/4/15 تاريخ القبول: 2024 /5/3 تاريخ النشر: 2024/5/15

الملخص:

تهدف هذه الدراسة إلى بيان كفاءة احترام البيانات الشخصية، حيث يتناول هذا البحث موضوع حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي؛ وذلك من خلال البحث عن النصوص والتشريعات العربية والأوروبية فى هذا الخصوص؛ مع الاسترشاد بالأحكام القضائية الصادرة عن القضاء الفرنسي والمغربي من أجل توفير الحماية اللازمة للبيانات ذات الطابع الشخص من الاعتداء عليها عبر شبكات مواقع التواصل الاجتماعي.

الكلمات المفتاحية: احترام البيانات الشخصية، مواقع التواصل الاجتماعي.

Abstract

This study aims to demonstrate the efficiency of respecting personal data, as this research addresses the issue of protecting the information privacy of the user through social networking sites. This is done by searching for Arab and European texts and legislation in this regard. Taking guidance from the judicial rulings issued by the French and Moroccan judiciary in order to provide the necessary protection for data of a personal nature from attack through social networking sites.

Keywords: respect for personal data, social networking sites.

Introduction

L'analyse juridique du concept ne nous retiendra guère. On sait qu'une jurisprudence classique ne réprimant l'atteinte à la vie privée que si son auteur avait commis une faute et que si sa victime avait éprouvé un préjudice. On s'accorde cependant aujourd'hui en jurisprudence et en doctrine à reconnaître dans le droit à l'intimité personnelle un droit subjectif et plus précisément un droit de la personnalité[1]. En outre le doyen Carbonnier professait sur la notion de la vie privée « la sphère secrète d'où il aura le pouvoir d'écarter les tiers, le droit d'être laisser- tranquille »[2].

Ce n'est pas l'atteinte à la vie privée, mais à « l'intimité » de la vie privée qui est plus restrictif, de telle sorte qu'on peut dire que le résultat est pratiquement le même. Le juge en exigeait une atteinte intolérable[3]. L'enquête s'efforce de privilégier les éléments qualitatifs et de suivre une démarche extensive; les pratiques à repérer sont à apprécier dans leurs aspects parfois contradictoires, c'est-à-dire en ce qu'elles constituent une garantie pour les individus mais également en ce qu'elles bloquent, parfois, le développement. Il est incontestable que les fichiers nominatifs suscitent des craintes, et les banques de données encore davantage. Cependant, on ne relève guère de plaintes motivées par des violations de la confidentialité et elles ne se sont nullement multipliées depuis l'emploi des ordinateurs. Il y a donc là une situation qu'il importe d'éclaircir[4].

Toutefois, dans la plupart des systèmes juridiques, les textes traditionnels qui intéressent les branchements d'écoute téléphonique clandestine et interceptions de communications de données, ne visent que l'interception des conversations ou communications orales[6], ils ne visent guère le traitement des données automatisées. Dans tous les pays, les difficultés que suscite l'application des dispositions pénales sont encore plus prononcées dans le domaine du simple accès non autorisé à des systèmes de traitement et de stockage des données. Le "simple" accès non autorisé à un ordinateur désigne le fait de s'y introduire sans causer à son propriétaire un dommage autre que celui d'acquérir connaissance des informations, sans but précis. C'est un acte comparable au fait de reproduire une clé ou de s'introduire chez autrui sans y causer le moindre dommages[7].

Par conséquent, la délinquance informatique est particulièrement difficile à réprimer, en droit parce que les infractions traditionnelles sont le plus souvent inadaptées aux comportements informatiques, en fait l'infraction informatique est complexe, technique, instantanée et souvent sans trace. C'est pourquoi de nouvelles infractions ont été imaginées par le législateur, dans le but de prévenir ces comportements attentatoires à l'intégrité des biens et des personnes[8]. il s'agit du principe incontournable de la vie privée envisagé à la protection des données personnelles (I) et leur étendu (II)

I : La protection des données personnelles comme principe au respect de la vie privée

La loi répressive innove hardiment, au profit de la personne physique, la protection de ses données personnelles. Contribue à protéger les données personnelles, la CNDP collabore avec la CNIL française et d'autres organismes internationaux, En amont du traitement, elle dispose d'un droit général à l'information, d'un droit de consentir et d'un droit d'opposition. Pendant le traitement, elle peut accéder aux données traitées, en demander la communication, la rectification et l'effacement. En cas d'atteinte à ses droits, elle peut déposer des plaintes, des réclamations ou pétitions et peut saisir les juridictions judiciaires. De fait, tout est mis en œuvre pour que l'intéressé se trouve en mesure d'exercer un contrôle sur les données le concernant qui sont traitées[9]. La protection assurée par le droit au respect de la vie privée à deux versants[10], Tout d'abord, elle permet de ne pas dévoiler des informations qui relèvent de la vie privée de la personne[11] et de sanctionner toute divulgation n'ayant pas donné lieu au consentement de l'intéressé (A). Elle permet en second lieu, que l'individu jouit d'une certaine liberté en ce qu'il peut vivre comme il l'entend, à l'abri des regards indiscrets[12] et donc édicter les dérogations à la collecte des données personnelles (B).

A- les conditions de la collecte des données personnelles

l'exigence de loyauté de la collecte ne peut être satisfaite que si la personne concernée en est informée (a), une collecte d'informations opérée par les responsables du traitement (b) à l'insu des personnes pouvant être considérée comme déloyale[13]

a- L'exigence du consentement de la personne concernée

Les détectives privés, ne disposant de pouvoir ni de perquisition ni d'arrestation, ne peuvent pas toujours mener l'enquête jusqu'au bout. Ils ont besoin de la collaboration de la police, une collaboration qui risque d'être refusée, car les enquêteurs de la police ont tendance à travailler à vase clos et sont frileux à l'idée de collaborer avec les gens du privé[14].

À travers ces constatations les enquêteurs privés peuvent à tout moment porter atteinte, dans le cadre de leurs missions, à la vie privée la personne concernée[15]. D'ailleurs l'article 4 de la loi 09-08[16] prévoit que le traitement des données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement à l'opération ou à l'ensemble des opérations envisagées. Il s'agit d'un consentement indubitable, ceci s'exprime à travers la révélation de l'identité du responsable du traitement, la destination des données ainsi que le droit d'accès et de modification des données. Faute de protéger véritablement la personne concernée, le consentement déresponsabilise le plus souvent le responsable de traitement sans offrir les garanties de prise de conscience recherchées[17]. Si le consentement ne permet pas toujours, en soi, de garantir la protection de la personne concernée, il n'offre pas non plus au responsable de traitement une véritable garantie pour sécuriser son traitement.

le consentement apparaît la base de traitement des données personnelles, le levier de l'interdiction de procéder aux données personnelles d'un assuré sans son consentement. Il serait déduit de manière exclusive une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière similaire ou significative[18]. Le consentement explicite de la personne concernée, l'assuré, dans ce cas, est stipulé en outre par l'article 447-1[19] du code pénal[20]. Il faut à cet égard souligner qu'il est envisagé ici *in fine* quoique l'on ne puisse en déduire aucune hiérarchie, conformément à ce qui a été souligné précédemment et dans des conditions distinctes que celles requises pour recueillir un consentement standard[21].

Le Dahir n° 1-14-175 du 21 rejeb 1441 (16 mars 2020)[22]garantit, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. Dans le domaine de la coopération policière et judiciaire, le consentement de la personne concernée tend à complètement s'effacer au profit d'un contrôle de la licéité du traitement des données quasi exclusif de l'autorité publique. La conception subjectiviste de la donnée est alors mise de côté, mais au-delà, le doute plane sur le maintien même, dans ce domaine, d'une catégorie de données personnelles dont la protection serait renforcée[23]. C'est le droit au respect de la vie privée, au sens strict, c'est-à-dire entendu comme le droit au respect de l'intimité qui sera ici préféré[24].

Chaque fois qu'il y a la sensibilisation des données traitées, l'assuré est en mesure d'exiger de véritables restrictions, particulièrement lorsqu'il s'agit des données sensibles, médicales ou judiciaires. Le consentement ne saurait être « standard »[25], ceci dit, la nécessité de garanties paraît indispensable pour la protection desdites données. Bien que dans un consentement traditionnel une telle volonté doit être libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à des fins de prospection directe[26]. De telles exigences peuvent être

manifestées et accomplies en remplissant un formulaire électronique, en envoyant un courrier électronique, en téléchargeant un document scanné porteur de la signature de la personne concernée ou en utilisant une signature électronique[27]. Un traitement de données à caractère personnel n'est licite que si, et dans la mesure où, il remplit au moins une condition[28], il s'agit aux termes de la loi 09-08[29] d'une obligation, suffisamment claire, stipulée par une disposition légale, car celle contractuelle ne pourrait fonder un tel traitement, ainsi qui ne peut s'appliquer que si elle mentionne la nature et l'objet du traitement[30]. L'objectif de cette règle est donc surtout d'empêcher que des données soient traitées de façon arbitraire, pour n'importe quelle finalité[31]

Plus délicate est, en revanche, la question de l'intérêt légitime énoncé aux termes des dispositions de l'article 4 al 2.5°[32], le traitement n'est légitime que si contribue à la réalisation d'un intérêt légitime, il pourrait exister lorsqu'il « existe une relation pertinente et appropriée avec la personne concernée ». L'intérêt doit être distingué de la finalité du traitement, alors que la finalité correspond au but ou à l'intention du traitement, l'intérêt s'entend de l'enjeu plus large poursuivi par le responsable du traitement, ou le bénéfice qu'il tire ou que la société pourrait tirer du traitement[33]. De ce point de vue, Les données à caractère personnel[34] doivent être sur demande du responsable du traitement et, s'il existe un intérêt légitime le responsable de traitement, en collectant et en stockant les données personnelles fait courir aux personnes concernées des risques de piratage et de divulgation non autorisée pouvant influer sur leur vie privée et leur porte préjudice[35]. Le consentement n'est pas un acquis de la protection, dans la mesure où certains traitements sont ou bien obligatoires ou simplement indispensables à une bonne gestion. Il est alors inconcevable on difficilement concevable d'en conditionner l'existence au bon voulu de l'individu[36].

b- Les obligations des responsables de traitement des données personnelles

L'article 12 de Déclaration universelle de droit de l'Homme stipule : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. ». Une claire stipulation de la constitution de 2011[37]à travers son article 24 qui énonce : « Toute personne a droit à la protection de sa vie privée, le domicile est inviolable, les perquisitions ne peuvent intervenir que dans les conditions et les formes prévues par la loi, les communications privées, sous quelque forme que ce soit, sont secrètes. Seule la justice peut autoriser, dans les conditions et selon les formes prévues par la loi, l'accès à leur contenu, leur divulgation totale ou partielle ou leur invocation à la charge de quiconque. Est garantie pour tous, la liberté de circuler et de s'établir sur le territoire national, d'en sortir et d'y retourner, conformément à la loi. En outre de la question de savoir si le responsable de traitement est tenu des obligations envers la personne concernée se pose la question de la notification préalable du traitement qu'il met en œuvre. Le responsable doit notifier à l'autorité de contrôle, avant sa mise en œuvre, tout traitement entièrement ou rationnellement automatisé ou tout ensemble de traitement de ce type ayant une finalité liée[38].

Trois conditions doivent être respectées pour que l'intérêt de la communication des données soit irresponsable, il est strictement demandé la légitimité, la réalité et la précision et la clarté. L'article 3 al 1- b, de la loi 09-08 relative au respect des données personnelles stipule « Les données à caractère personnel doivent être collectées pour des finalités déterminées explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec finalités » ceci dit, l'intérêt doit être « acceptable au regard du droit »[39]

En outre l'article 3 al 2 appréhende que les données personnelles ne pourraient être que sur demande du responsable et s'il existe un intérêt légitime. Alors sans un intérêt légitime le responsable n'est pas tenu d'une telle demande, cependant, la prévention de la fraude est susceptible d'être invoquée parmi les exigences de l'intérêt légitime qui donne droit au responsable

d'y accéder. Le responsable de traitement et le sous-traitant voient leur régime de responsabilité s'aligner de sorte que le second ne sera plus en mesure de diluer sa propre responsabilité derrière le premier. Ils seront tous les deux responsables en cas de violations des dispositions de la règlementation Informatique et Libertés. Par ailleurs, la responsabilité pénale personnelle du dirigeant pourra dans certains cas être engagée[40].

Le responsable de traitement a collecté des données pour certaines finalités, telles que décrites dans la déclaration ou dans la demande d'autorisation. Maintenant qu'il en dispose, il lui est interdit d'utiliser ultérieurement ces données de manière incompatible avec ces finalités[41]. L'article premier de la loi 09-08 al 1 délimite le champ d'application des données à caractère personnel, il s'agit de toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable, dénommée ci-après « personne concernée ». L'article 7 de la loi 09-08 énonce à l'égard du droit d'accès « La personne concernée, justifiant de son identité, a le droit d'obtenir du responsable du traitement, à des intervalles raisonnables, sans délais et gratuitement : a) la confirmation que les données à caractère personnel la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte, et les destinataires ou les catégories de destinataires auxquels les données à caractère personnel sont communiquées ; b) la communication, sous une forme intelligible, des données, à caractère personnel faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données. Le responsable du traitement peut demander à la Commission nationale des délais de réponses aux demandes d'accès légitimes et peut s'opposer aux demandes manifestement abusives, notamment, par leur nombre et leur caractère répétitif. En cas d'opposition, la charge de la preuve du caractère manifestement abusif, incombe au responsable du traitement auprès duquel ces demandes ont été faites. c) La connaissance de la logique qui sous-tend tout traitement automatisé des données à caractère personnel la concernant ».

B- les dérogations à la collecte des données personnelles

a- Délimitation du champ de la collecte

Lorsqu'une entité décide de mettre en place un système de collecte de données personnelles, elle est tenue de préciser l'objectif de cette collecte. Parmi les exemples fréquents, celui des cookies est assez emblématique : il s'agit de la notification sur un site internet qui demande à l'internaute son consentement pour collecter des informations sur sa navigation, généralement dans le but de lui proposer des contenus et publicités personnalisés[42]. C'est au regard de la finalité du fichier que s'apprécient le caractère adéquat, pertinent et non excessif des données collectées, la durée pendant laquelle les informations peuvent être conservées ou encore les destinataires de ces informations[43]. la Commission nationale de contrôle de la protection des données à caractère personnel(CNDP) exige la notion du consentement dans la protection des données, Le traitement des données, à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement à l'opération ou à l'ensemble des opérations envisagées[44].

En vertu de l'article 3 al I-(b)-de la loi 09-08 , les données à caractère personnel doivent être: collectées pour des finalités déterminées explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec finalités ; (c) adéquates, pertinentes et non excessives, au regard des finalités pour lesquelles elles sont collectées, et pour lesquelles, elles sont traitées ultérieurement; (d)Toutes les mesures raisonnables doivent être prises, pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles, sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

Toute finalité secrète ou implicite doit être rejetée, de même que les traitements mis en œuvre à toutes fins utiles. L'exigence s'incarne dans des obligations particulières imposées au responsable du traitement, notamment celles d'informer la personne concernée au sujet du traitement et de notifier celui-ci à l'autorité de contrôle, elle répond à des objectifs concrets. Il s'agit de rendre possible le contrôle du traitement, la finalité se présente en effet comme le critère central de la vérification du respect de la protection instaurée, tant le contrôle de la légitimité de la finalité que celui de la conformité des données traitées à cette dernière supposée

L'article premier stipule « Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires, le responsable du traitement doit être indiqué dans la loi d'organisation et de fonctionnement ou dans le statut de l'entité légalement ou statutairement compétente pour traiter les données à caractère personnel en cause ». la finalité doit permettre d'apprécier la pertinence des données traitées, leur proportionnalité, ainsi que celle de la durée de conservation, de déterminer les destinataires et de manière plus générale de fixer le cadre légal et réglementaire applicable, lequel ne se limite pas à la seule application de la loi Informatique et libertés[45]. D'après une doctrine « le Régulateur vise aujourd'hui les "données à caractère personnel" non plus tant par rapport à la personne sur laquelle elles portent mais par rapport à l'usage qui en est fait, ou pour lequel la "donnée" a été prélevée, traitée et conservée[46]. Cette affirmation témoigne du besoin que ressent la doctrine, pour comprendre l'évolution de la donnée à caractère personnel, de s'intéresser à la réalité des traitements et non plus seulement à la notion abstraite de donnée à caractère personnel[47].

Le principe de finalité est la « colonne vertébrale »[48] de la loi 09-08 . Il n'est pas possible de collecter des données au cas où, la finalité étant le point de référence, l'étalon de mesure du danger pour les droits et libertés résultant du traitement de données à caractère personnel[49]. Seul un contrôle strict de la finalité des traitements et une répression sans faiblesse doivent permettre d'éviter une utilisation arbitraire et sans limites des innombrables possibilités que l'informatique offre en matière d'exploitation d'informations nominatives[50]. Célèbres auteurs ont enseigné que le but même de la protection des données -le respect des libertés et des droits fondamentaux de l'individu - implique qu'une finalité de traitement ne peut violer sans justification légitime ces droits et libertés. C'est pourquoi la finalité poursuivie doit être utile et nécessaire au vu de l'objet social de l'entreprise ou de l'intérêt général. Elle ne peut non plus provoquer une ingérence excessive dans les libertés individuelles. Il convient en effet de mettre en balance l'intérêt des individus concernés à voir préserver leurs droits et libertés, et l'intérêt public ou privé à procéder au traitement des données[51].

Le responsable de traitement qui détient des données à caractère personnel ne peut détourner ces informations de leur finalité lors de leur enregistrement, leur classement, leur transmission ou toute autre forme de traitement[52]

L'article 54 de la loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel envisagé l'emprisonnement de trois mois à un an et d'une amende de 20.000 à 200.000 DH ou de l'une de ces deux peines seulement quiconque, met en œuvre un traitement à des fins autres que celles déclarées ou autorisées ou soumet les données précitées à un traitement ultérieur incompatible avec les finalités déclarées ou autorisées. Ainsi la conservation excessive des données personnelles, le détournement de finalité sont autant d'infractions pénales qui ne peuvent être rendues licites par le consentement de la personne concernée. Si le consentement de la victime tend de plus en plus à être pris en compte dans la constitution des infractions pénales[53], il n'a qu'une faible place parmi les incriminations pénales tendant à garantir le respect de la réglementation en matière d'utilisation des données personnelles.

Le consentement ne permet pas de rendre licite ces infractions en s'opposant à leur constitution ou en étant une condition de leur justification. Ces sanctions pénales tendant à garantir le respect de la réglementation en matière d'utilisation des données personnelles constituent ainsi des dispositions d'ordre public[54].

b- L'interdiction de l'enregistrement des données sensibles

Il est clair que l'informatique altère dès maintenant en profondeur certains mécanismes juridiques traditionnels. Ceci est particulièrement net lorsqu'une opération quelconque a pour support un instrument écrit[55]. On observe qu'en vertu de son droit d'accès aux données, l'assuré peut notamment demander à être informé sur la logique qui sous-tend tout traitement automatisé de prise de décision. L'objectif est d'accroître l'effectivité de la protection contre les décisions automatisées. Selon certains auteurs, le responsable devrait aussi informer l'intéressé sur la logique sous-tendant des décisions mixtes (partiellement automatisées), afin que le prescrit légal ne soit pas vidé de sa substance et que la personne concernée ait effectivement la possibilité d'exercer ses droits[56]. L'interdiction de prendre une décision sur le seul fondement d'un traitement automatisé est levée soit lorsque cette décision est prise dans le cadre d'un contrat entre le responsable et la personne concernée, soit lorsqu'elle est fondée sur une disposition légale. Le recours à l'informatique, dans une recherche pénale, suppose une standardisation particulièrement forte dont il faut bien peser, chaque fois, les avantages et les inconvénients, les gains et les pertes[57]. Pour les investigateurs, l'exploitation du matériel informatique, qu'il s'agisse d'ordinateurs ou de supports de stockage, constitue une étape essentielle vers la manifestation de la vérité. Toutefois, l'obstacle majeur dans cette opération réside dans l'exploitation du support informatique par une personne étrangère à l'enquête. En effet, au sein de la masse d'informations recueillies, il est indispensable de savoir quelles données sont susceptibles de faciliter l'administration de la preuve de la commission de l'infraction[58].

Il est aussi difficile de déterminer la portée de l'interdiction de l'enregistrement des informations nominatives relatives aux infractions et aux condamnations pénales[59]ainsi qu'au sureté publique. L'État est obligé de protéger pour chaque individu le libre développement de son activité physique et intellectuelle. Il doit garantir à chacun la liberté individuelle, par des mesures préventives et répressives, mesures qui sont elles-mêmes une restriction de la liberté individuelle, mais qui sont légitimes si elles sont les mêmes pour tous et si elles n'ont pour but et pour limites que la nécessité de protéger la liberté individuelle de tous. Toute législation positive doit organiser un système garantissant puissamment la liberté individuelle[60].

Cependant, aucun texte de loi marocaine ne parvient à régir le traitement automatisé d' informations nominatives relatif aux infractions, les condamnations ou mesures de sûreté. Les dispositions de La loi 07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données procède à une interprétation large desdites données. « Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé »[61]. Or, une panoplie de lois régissant la matière ont été bien élaborées par le législateur français. D'ailleurs, deux textes de loi, avec une même fin, ont été adoptés successivement il s'agit de l'article 31 al 1 de la loi du 6 janvier 1978[62] qui dispose « Sauf dispositions législatives contraires, les juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la commission nationale, les personnes morales gérant un service public peuvent seules procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté » ainsi que l'article 6 de la loi 80-2 du 4 janvier 1980[63] étendant l'application de la règle établie par la première loi, stipulant « Aucun fichier ou recueil de données nominatives détenu par une personne quelconque ou par un service de l'État ne dépendant pas du ministère de la justice ne pourra mentionner, hors les cas et dans les conditions prévus par la loi, des jugements ou arrêts de condamnation ».

L'accès est considéré comme une infraction dès lors qu'il est opéré de manière frauduleuse, c'est-à-dire sans droit, le simple fait d'avoir outrepassé un système de sécurité existant est constitutif d'un accès frauduleux. Toutefois, la loi n'impose

pas la mise en place d'un dispositif de sécurité pour sanctionner un tel agissement[64]. La Cour de Paris ne dit pas autre chose[65] « L'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers d'un système, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il a si procède à distance ou qu'il se branche sur une ligne de télécommunication». Le simple fait d'entrer est incriminable, comme l'a rappelé encore la Cour d'appel de Toulouse[66] « L'accès à un système informatisé de données tombe sous le coup de la loi pénale dès lors qu'il est le fait d'une personne qui n'a pas le droit d'y accéder, importante et réelle soit donnée aux citoyens afin qu'ils puissent être capables de contrôler eux-mêmes l'emploi des renseignements qui sont recueillis auprès d'eux, d'en discuter et d'en contrôler l'usage.

La nouvelle loi offre un cadre de protection pour les libertés individuelles encore faudrait-il que les individus soient rendus conscients qu'ils ont des libertés et des droits à protéger et à faire valoir et que les moyens leur soient donnés pour exercer réellement ce contrôle[67]. L'exercice de ce droit implique, en effet, que les résultats d'un traitement automatisé sont opposés à une personne », quel que soit l'objet de ce traitement. Cette personne a dans ce cas le droit de connaître et de contester, à la fois les informations, et les raisonnements utilisés par le traitement. Ce droit n'est donc pas limité aux informations nominatives, il ne peut en revanche être exercé qu'à l'égard des traitements automatisés[68].

L'interprétation des textes de loi implique des exceptions à l'interdiction de l'enregistrement des informations nominatives relatives aux infractions, condamnations et mesures de sûreté. Le droit à l'information ne peut être limité que par la loi, dans le but d'assurer la protection de tout ce qui concerne la défense nationale, la sûreté intérieure et extérieure de l'État, ainsi que la vie privée des personnes, de prévenir l'atteinte aux droits et libertés énoncés dans la présente Constitution[69].

II- l'étendue de la protection des données personnelles

L'étendue de la protection n'est pas toujours la même car elle dépend de son but, elle peut avoir pour fin, et c'est la situation la plus fréquente, de protéger le secret de la vie privée des personnes[70] contre des investigations (A) et à l'opposé de la divulgation de certaines de ces données (B).

A- La protection contre les investigations des données personnelles

a- L'enregistrement des paroles et de l'image

La jurisprudence, perpétuellement, protège les personnes contre l'exploitation de leur personnalité, c'est-à-dire contre l'utilisation à une fin lucrative, sans leur autorisation , d'un élément de leur personnalité, nom, image, voix, événement de la vie privée[71]. L'espionnage de la parole ou de l'image d'autrui n'est répréhensible que si plusieurs conditions sont réunies. Les agissements doivent en effet avoir pour cadre un lieu privé et leur auteur doit avoir eu l'intention de porter atteinte à l'intimité de la personne espionnée. Très logiquement en outre, les faits doivent avoir été accomplis sans le consentement de celle-ci[72], tel édicté par l'article 447-1 du code pénal[73].

Le consentement de la victime, en revanche, fait disparaître l'infraction. Il s'agit d'une exception au principe applicable en droit pénal selon lequel l'accord de la victime ne constitue pas un fait justificatif[74], sauf pour les infractions pour lesquelles l'absence de consentement constitue un élément de l'infraction (ce qui ne recouvre pas fatalement les cas de délits privés pour lesquels le caractère privé conditionne la poursuite à une plainte de la victime, mais pas l'existence de l'infraction, par exemple la diffamation).[75] Il s'agit donc d'un délit qui porte atteinte à l'intimité de la vie privée, qui s'étend chaque fois l'auteur de l'acte s'estimait à l'abri au regard des tiers, cette intimité est veillée dès lors que l'image d'une personne a été prise sans son consentement ou à son insu[76]

L'exigence d'une preuve de consentement est difficilement applicable dans la pratique car elle suppose qu'avant chaque prise de photographie ou avant un enregistrement une autorisation écrite soit donnée par la personne concernée[77]. Une précision nous semble devoir être apportée qui concerne aussi bien les appareils concernant le son que ceux concernant l'image il n'est même pas nécessaire qu'ils soient utilisés en vue de surprendre l'intimité de la vie privée[78].

Afin d'assurer la protection d'intérêts légitimes et notamment « la protection de la réputation et des droits d'autrui », il n'en demeure pas moins que la liberté est la règle et que la restriction est l'exception[79]. Ainsi, certains auteurs estiment-ils qu'il y a lieu d'opérer une distinction et préfèrent considérer que le droit à l'image est indépendant du droit au respect de la vie privée. Il est vrai que parfois une atteinte à l'image d'une personne n'entraînera pas nécessairement une atteinte à la vie privée[80]. Plusieurs fondements ont été proposés pour justifier la protection du droit à l'image : la propriété, le respect de la vie privée et la protection de la personnalité. Mais, dans l'analyse devenue aujourd'hui classique, l'on préfère fonder directement le droit à l'image sur les seuls droits de la personnalité[81]. L'atteinte portée au sujet de l'image s'accompagne en effet d'une violation manifeste du droit à l'information et d'une véritable trahison de la confiance du public[82].

Sans doute, doit-on appliquer le principe « *noli me tangere* » non seulement au corps humain, mais aussi à sa spiritualisation : l'individualité du sujet ; de même, faut-il « poser en principe le droit, pour l'intéressé, de faire reconnaître sa personnalité et de la développer, de revendiquer les caractères qui l'individualisent, de ne pas vouloir laisser altérer sa personnalité contre son gré »[83]. L'altération d'une personnalité lors de la représentation tangible de l'image d'une personne doit être définie comme toute modification de ses traits physiques, intellectuels, moraux, qui trahit la réalité de son être concret[84].

J. PRADEL dans une conclusion d'un arrêt de la cour de cassation admettait que si une information est ouverte, l'écoute téléphonique est licite. La jurisprudence l'admet d'ailleurs tant à l'égard d'une personne inculpée formellement[85] qu'à l'égard des témoins[86]; et cette jurisprudence nous paraît justifiée. Si une information n'est pas ouverte, il n'y a pas de jurisprudence et la licéité de l'écoute reste douteuse[87]. La sauvegarde du secret, remarque-t-on, pose une condition de la confiance entre les citoyens et, si paradoxal que cela puisse paraître, facilite la communication de la vérité en supprimant la nécessité de la dissimulation[88].

Bref on pourrait s'inspirer du modèle allemand[89], « l'écoute ne peut être ordonnée que par un juge (ou en cas d'urgence par le procureur de la République, à charge pour celui-ci de saisir le juge dans les trois jours); et elle ne peut être décidée que dans certains cas tels les atteintes à la sûreté de l'Etat, les actes de terrorisme, les prises d'otage, les assassinats, les vols à main armée. On a de plus en plus intérêt à consulter les législations étrangères[90]

b – Le droit à l'inviolabilité du domicile

Nous ne pouvons, ici, donner une énumération limitative des hypothèses où le législateur a donné à certains fonctionnaires des pouvoirs de contrôle et d'investigation leur permettant de pénétrer dans le domicile des particuliers, même contre leur volonté. Ils ne peuvent, en tout cas, y pénétrer (sauf état de nécessité pour porter secours éventuel) que dans les cas se rattachant à la commission, réelle ou éventuelle, d'une infraction et dans les conditions précisées par la loi[91].
Le droit à l'inviolabilité du domicile est consacré par l'article 441 c.p[92].

L'inviolabilité, par sa simple acception grammaticale, évoque, dans la langue courante, l'idée d'un acte négatif. Il en est de même dans le langage juridique, où elle consiste en la défense de porter atteinte à la liberté humaine, défense qui vise à

la fois l'autorité et les particuliers et qui se résout en la reconnaissance de deux libertés : liberté de la personne physique, liberté du domicile[93].

Toutes les fois qu'un rapport quelconque s'est effectivement établi entre une personne et un lieu, ce dernier participe de la qualité inviolable attachée à la personne. Peu importe que le rapport en question soit essentiellement éphémère du moment qu'il est réel[94], le domicile ne sera pleinement protégé que si la jurisprudence comprend assez largement cette notion de violence[95].

Dans l'absolu, une simple affaire pénale pourrait générer une myriade d'investigations de sources différentes. Or aucun système pénal de culture hiérarchique n'adhère à une telle croyance. Au sein d'un tel système, c'est uniquement à l'autorité publique qu'il incombe de rechercher la vérité car, contrairement aux particuliers, elle seule est tributaire de cette mission: viser l'intérêt général[96]. Le délit de violation du domicile commis par un particulier figure dans la section « des atteintes portées par des particuliers à la liberté individuelle, de la prise d'otages et de l'inviolabilité du domicile du code pénal »[97].

Une violation de domicile peut très bien avoir lieu sans qu'il n'y ait aucune atteinte portée à la vie privée. Ceci ne signifie nullement que la protection de la vie privée soit de ce fait poursuivie à titre secondaire. Cette finalité est aussi importante que les autres si ce n'est plus parfois[98].

La violation du domicile exige le fait que l'introduction ait eu lieu contre le gré c'est-à-dire sans le consentement de l'habitant. En outre, du moment que l'introduction d'un agent de l'autorité dans le domicile d'un citoyen constitue le délit de violation de domicile sans qu'il y ait lieu de s'occuper des moyens employés par cet agent pour y parvenir, l'introduction d'un simple particulier dans le domicile d'un autre particulier n'est punissable comme violation de domicile que lorsqu'elle a eu lieu « à l'aide de menaces ou de violences »[99]. La jurisprudence interprète assez largement ces termes et sanctionne ainsi tout procédé permettant de s'introduire dans un domicile contre la volonté ou sans consentement de son occupant[100].

Malgré les apparences, la propriété d'autrui reste encore une valeur protégée, mais d'une protection soumise à la stricte application du droit[101]. Quel est donc le sens exact interpellé par la loi répressive en vertu de son article 441[102] qui mettent en cause la responsabilité des enquêteurs privés à l'égard de l'individu profane ? Les expressions « fraude », « menaces » ou « violences », délimitent les éléments qui peuvent engager la responsabilité des auteurs de l'infraction. P. CASSAGNE a largement établi une signification de « menaces » et « violences » dans la mesure où le législateur s'est contenté des deux expressions. La signification du mot « menaces » n'a jamais donné lieu à aucune discussion. Ce mot désigne, évidemment, tout moyen d'intimidation employé sur la personne de l'habitant pour le contraindre à ouvrir les portes de son logement. L'emploi de ce moyen suppose donc, qu'au moment où se commet le délit, l'habitant est effectivement présent dans son domicile. Le mot « violences » a donné lieu, au contraire, à une difficulté d'interprétation[103].

Le maintien frauduleux ne suppose pas une introduction préalable irrégulière. L'énumération textuelle des moyens de commettre l'infraction est suffisamment large pour englober tous les cas d'introduction ou de maintien dans le domicile d'autrui par un procédé malhonnête[104].

L'infraction est intentionnelle. Elle suppose la conscience de l'absence d'autorisation à entrer ou à se maintenir dans le lieu privé L'infraction ne sera donc pas retenue lorsque l'occupant ne s'est pas opposé à la présence de l'agent ou a donné son accord. La preuve de l'élément moral est aisément déduite des faits dans la mesure où ceux-ci supposent l'accomplissement de manœuvres, de voies de fait ou l'usage de menaces ou de contrainte[105], il ne fait aucun doute qu'en concevant le domicile comme tout lieu où la personne a le sentiment d'être chez elle sans aucune autre condition, la jurisprudence a donné comme

finalité à ces délits de protéger à travers ce domicile la vie privée qu'il abrite. Mais bien que très important, cet objectif n'est cependant pas le seul à être poursuivi par ces incriminations puisque celles-ci assurent en même temps la défense des droits de toute personne à la tranquillité et à la sécurité[106]

B– La protection contre la divulgation de la vie privée

a- Les atteintes au secret des correspondances

Il semblerait naturel, au premier abord, que l'inviolabilité de la correspondance, avec des bases aussi sacrées que la liberté de la pensée et la propriété, fût de tout temps respectée. Ce principe que l'on se figure en théorie à l'abri de toute atteinte a été dans la pratique trop souvent foulé aux pieds[107]. C'est le cas, parmi les premiers, des délits de violation des correspondances, qui protègent non seulement la liberté d'expression de la pensée par la correspondance, mais aussi les secrets de la vie privée qu'elle contient souvent[108].

La notion de correspondance au sens de l'article 8 de la Convention européenne des droits de l'homme n'est certes pas limitée aux lettres missives. Elle recouvre au contraire toutes les formes de communication, qu'elles soient orales ou écrites, et quel que soit le moyen de communication utilisé : téléphone fixe ou mobile , courrier électronique , SMS , etc. L'enregistrement à distance de conversations tenues en pleine rue pourrait donc aussi constituer une ingérence dans le droit au respect de la « correspondance ». Plus généralement, tant l'écoute que l'enregistrement des conversations portent atteinte au secret de la « correspondance ». De même, détecter les caractéristiques des liaisons téléphoniques (durée , périodes, heures , etc.) c'est aussi s'immiscer dans le secret de ladite correspondance.

Mais il ne suffit pas de poser le principe de l'inviolabilité, il fallait encore en assurer le respect. Pour atteindre ce but, le législateur n'a pas hésité à sanctionner pénalement la prise de conscience du secret, malgré des hésitations, des retours en arrière, la sévérité du système répressif s'est progressivement accrue[109]. La suppression vise tous les agissements malveillants susceptibles de priver, même momentanément, les destinataires, des correspondances qui leur sont adressées[110]. Le spectre de cette protection, qui vise au premier chef, à préserver la vie privée de tout auteur d'une correspondance, déborde néanmoins cette notion. La meilleure preuve en est que les textes incriminations ne mentionnent pas le terme « privé », si bien qu'il n'est pas possible de réduire le champ d'application de ce secret aux seules correspondances contenant des éléments relatifs à la vie privée[111].

Un premier point ne fait aucun doute, jurisprudence et auteurs considèrent la lettre comme un meuble susceptible de transmission et de possession, à l'exemple des livres, manuscrits et registres domestiques[112] classiques reposent sur un support tangible. Dans ce registre, elles peuvent être de toute nature, quel que soit leur mode d'acheminement ou de délivrance?, lettres quelconques, messages ou plis, fermés ou non comme une carte postale Cette interprétation est tout à fait conforme à la *ratio legis* de l'incrimination, à savoir à confiance dans la confidentialité et la sécurité des correspondances condition de la liberté de la communication[113]. Les correspondances ayant un support papier, la référence à la nature du support permet tout naturellement d'exclure les correspondances qui, quoique écrites, trouvent élection dans un autre support et qui, cela allant de pair, empruntent des voies d'acheminement liées aux télécommunications[114].

L'atteinte aux correspondances est admise, pour la Cour de cassation française, dans l'ouverture ou la suppression intentionnelle de toute correspondance adressée à des tiers, de telle sorte que le secret en a été violé quand le destinataire a été privé définitivement ou temporairement de l'écrit à lui expédié[115]. Le code pénal marocain consacre une interprétation plus

large des atteintes portées à l'honneur et à la considération des personnes et de la violation des secrets, en annonçant l'inviolabilité des correspondance en vertu de son article 448 « quiconque, hors les cas prévus à l'article 232[116], de mauvaise foi, ouvre ou supprime des lettres ou correspondances adressées à des tiers, est puni de l'emprisonnement d'un mois à un an et d'une amende de 200 à 500 dirhams ou de l'une de ces deux peines seulement ».

Ce secret est circonscrit aux correspondances revêtant un caractère « personnel », c'est-à-dire celles adressées à une personne ou à un groupe de personnes individualisées, et ne bénéficie qu'au destinataire de la correspondance[117]. C'est le cas de la compagnie d'assurance qui poursuit un assuré suspect de blanchiment de capitaux en violant son adresse mail par des procédés des responsables de traitement.

Les termes de l'article 448 du code pénal exige nettement que la correspondance soit adressée à un tiers. La qualité de tiers ne pose apparemment pas de difficulté et, en application de cette condition, ne sont pas protégées les correspondances qui ne sont pas adressées à une personne en particulier[118].

Faut-il alors en conclure diverses situations qui peuvent être incriminées électroniquement étant donnée la technologie juridique récente. le fait de procéder à l'installation d'appareils (auxquels il faut sans doute assimiler aujour d'hui les logiciels) de nature à permettre l'interception de telles correspondances ce qui revient à incriminer un acte préparatoire; le fait d'intercepter et de détourner des correspondances émises, transmises ou reçues par voie électronique, il n'est pas néces saire que l'agent ait pris connaissance des propos tenus; le fait d'utiliser ces mêmes correspondances, ce qui implique la prise en compte de leur contenu; le fait de divulguer ces mêmes correspondances, cela couvre aussi bien la communication à un tiers que la communication à un ensemble indéterminé de personnes[119].

Peu importe le procédé utilisé dès lors que des signaux sont effectivement transmis par voie électromagnétique[120]. En toute hypothèse, le procédé peut être automatisé. Il suffit qu'un appareil » intercepte ou détourne la correspondance conformément à la volonté de celui qui l'a installé ou fait installer[121]

b- les éléments constitutifs des atteintes au secret des correspondances

L'article 12 de la déclaration universelle des droits de l'Homme énonce : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». À l'instar de la violation de domicile, le délit portant sur les correspondances présente ainsi deux aspects différents suivant qu'il est le fait d'un fonc tionnaire ou d'un particulier[122].

Le délit du particulier ne se conçoit en effet que s'il a agi « de mauvaise foi » et le législateur souligne encore spécialement cette disposition d'esprit malhonnête au sujet de la prise de connaissance qui doit être faite « frauduleusement ». Concrètement, ces précisions signifient que le juge devra expressément constater qu'avant d'ouvrir ou de supprimer la lettre, l'agent savait qu'elle ne lui était pas destinée[123].

Le législateur incrimine ainsi non seulement le fait d'ouvrir et, éventuellement, de prendre connaissance de correspondances adressées à des tiers ; mais aussi le fait de supprimer, de retarder ou de détourner ces correspondances. Peu importe alors qu'elles aient été ouvertes ou non. Dans la première hypothèse, l'incrimination tend à garantir la confidentialité de la correspondance ; dans la seconde hypothèse, elle tend à garantir son bon acheminement[124].

En outre, cette exigence d'une mauvaise foi appelle deux remarques complémentaires, d'une part, les juges doivent rechercher si l'intention de l'agent a seulement été de supprimer, d'ouvrir ou de détourner une correspondance ou si, comme

c'est quelquefois le cas, elle n'allait pas au-delà. Il semble en particulier qu'en cas d'appropriation du contenu d'une correspondance dans le but d'en tirer profit la qualification de vol soit plus adéquate. D'autre part, la mauvaise foi de l'agent tombe devant certaines causes d'irresponsabilité pénale[125].

Le simple fait de l'ouverture volontaire suffit pour que le délit soit constitué[126]. Un acte de rétention volontaire, même de courte durée, suffit à constituer la violation de correspondance et que , d'autre part , le fait de photographier ou photocopier les mentions portées sur l'enveloppe d'une lettre en cours de transmission ou sur les cartes ou correspondances circulant à découvert constitue une véritable appropriation de ces textes et ce , en violation du principe du secret des correspondances[127].

Avec le développement rapide du SaaS (Software As A Service) les entreprises se posent légitimement la question de la sécurité de leurs données dans le Cloud. Si le problème est souvent examiné en terme technique de sécurité physique des données, il doit aussi l'être en matière de sécurité juridique de données parfois très sensibles. Le recours au Cloud computing peut nuire à la sécurisation des données personnelles en créant notamment des risques de dispersion et de dépossession. Un manque d'étanchéité des données entre clients et une perte de confidentialité sont redoutés[128]

Moralement, le respect du secret de la correspondance privée s'impose aux particuliers et leur interdit de livrer à la publicité les lettres dont ils ne sont pas propriétaires : « Le secret des lettres est un principe que la justice ne peut méconnaître et qui s'impose autant à la morale publique qu'à la sûreté des relations privées »[129]. « L'inviolabilité du secret des lettres est un principe de haute moralité qui intéresse essentiellement l'ordre public[130]

À bien des égards entre les diverses infractions, les termes de l'article 448 du code pénal conçoit la mauvaise foi de l'auteur, l'intention suppose la connaissance que la correspondance est destinée à un tiers et le caractère volontaire de la violation[131]. Ce qui exclut en cas d'erreur de fait ; comme de règle, le mobile est sans importance[132]. Le contenu intellectuel et moral d'une correspondance remise à son destinataire peut revêtir un caractère tout particulier et confidentiel susceptible d'apporter des restrictions au droit de propriété reconnu au destinataire sur les lettres missives et d'ouvrir ainsi, au profit de l'auteur notamment, un droit au secret garantissant, avec la paix publique, la personnalité de l'auteur[133]. Quel que soit l'intérêt soulevé par les problèmes de droit pénal en cette matière, c'est dans le domaine du droit civil que , dans la pratique , la violation du secret des correspondances pose les questions les plus délicates[134] Cela tient d'abord au fait que la jurisprudence rattache le principe de l'inviolabilité du secret à la théorie des droits de la personnalité et lui assigne comme fondement la personne même dont il est destiné à assurer la protection[135]

La personne qui, sachant qu'elle n'y est pas autorisée, se maintient dans un système de traitement automatisé de données ». Cela semble parfaitement justifié : le statut d'administrateur réseau ne permet pas un espionnage généralisé des correspondances. L'administrateur réseau remplit une fonction particulière et abuse de cette fonction chaque fois qu'il la détourne à des fins personnelles. Il n'est pas alors dans une situation différente d'un tiers espion. Une telle interprétation paraîtra exagérée à certains mais elle se justifie par le fait que le législateur n'incrimine pas seulement l'introduction sans droit dans un système, mais aussi le fait de s'y maintenir. Or, en cas de détournement, les droits d'origine sont nécessairement perdus. Le maintien s'avère alors frauduleux[136], on pourrait le contester en relevant que le respect des correspondances implique alors une action plutôt qu'une abstention, voire qu'il fait assumer au réceptionnaire un rôle dans la distribution du courrier qui n'est pas le sien. Néanmoins, les termes de l'incrimination sont suffisamment généraux pour permettre cette interprétation[137]

Ce n'est donc pas l'extension du fait justificatif tiré du respect des droits de la défense qui est condamnée en l'espèce, ce sont ses conditions d'existence qui sont mises en doute[138].

b- les éléments constitutifs des atteintes au secret des correspondances

L'article 12 de la déclaration universelle des droits de l'Homme énonce : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ». À l'instar de la violation de domicile, le délit portant sur les correspondances présente ainsi deux aspects différents suivant qu'il est le fait d'un fonctionnaire ou d'un particulier[139].

Le délit du particulier ne se conçoit en effet que s'il a agi « de mauvaise foi » et le législateur souligne encore spécialement cette disposition d'esprit malhonnête au sujet de la prise de connaissance qui doit être faite « frauduleusement ». Concrètement, ces précisions signifient que le juge devra expressément constater qu'avant d'ouvrir ou de supprimer la lettre, l'agent savait qu'elle ne lui était pas destinée[140].

Le législateur incrimine ainsi non seulement le fait d'ouvrir et, éventuellement, de prendre connaissance de correspondances adressées à des tiers ; mais aussi le fait de supprimer, de retarder ou de détourner ces correspondances. Peu importe alors qu'elles aient été ouvertes ou non. Dans la première hypothèse, l'incrimination tend à garantir la confidentialité de la correspondance ; dans la seconde hypothèse, elle tend à garantir son bon acheminement[141].

En outre, cette exigence d'une mauvaise foi appelle deux remarques complémentaires, d'une part, les juges doivent rechercher si l'intention de l'agent a seulement été de supprimer, d'ouvrir ou de détourner une correspondance ou si, comme c'est quelquefois le cas, elle n'allait pas au-delà. Il semble en particulier qu'en cas d'appropriation du contenu d'une correspondance dans le but d'en tirer profit la qualification de vol soit plus adéquate. D'autre part, la mauvaise foi de l'agent tombe devant certaines causes d'irresponsabilité pénale[142].

Le simple fait de l'ouverture volontaire suffit pour que le délit soit constitué[143]. Un acte de rétention volontaire, même de courte durée, suffit à constituer la violation de correspondance et que , d'autre part , le fait de photographier ou photocopier les mentions portées sur l'enveloppe d'une lettre en cours de transmission ou sur les cartes ou correspondances circulant à découvert constitue une véritable appropriation de ces textes et ce , en violation du principe du secret des correspondances[144].

Avec le développement rapide du SaaS (Software As A Service) les entreprises se posent légitimement la question de la sécurité de leurs données dans le Cloud. Si le problème est souvent examiné en terme technique de sécurité physique des données, il doit aussi l'être en matière de sécurité juridique de données parfois très sensibles. Le recours au Cloud computing peut nuire à la sécurisation des données personnelles en créant notamment des risques de dispersion et de dépossession. Un manque d'étanchéité des données entre clients et une perte de confidentialité sont redoutés[145]

Moralement, le respect du secret de la correspondance privée s'impose aux particuliers et leur interdit de livrer à la publicité les lettres dont ils ne sont pas propriétaires : « Le secret des lettres est un principe que la justice ne peut méconnaître et qui s'impose autant à la morale publique qu'à la sûreté des relations privées »[146]. « L'inviolabilité du secret des lettres est un principe de haute moralité qui intéresse essentiellement l'ordre public[147]

À bien des égards entre les diverses infractions, les termes de l'article 448 du code pénal conçoit la mauvaise foi de l'auteur, l'intention suppose la connaissance que la correspondance est destinée à un tiers et le caractère volontaire de la

violation[148]. Ce qui exclut en cas d'erreur de fait ; comme de règle, le mobile est sans importance[149]. Le contenu intellectuel et moral d'une correspondance remise à son destinataire peut revêtir un caractère tout particulier et confidentiel susceptible d'apporter des restrictions au droit de propriété reconnu au destinataire sur les lettres missives et d'ouvrir ainsi, au profit de l'auteur notamment, un droit au secret garantissant, avec la paix publique, la personnalité de l'auteur[150]. Quel que soit l'intérêt soulevé par les problèmes de droit pénal en cette matière, c'est dans le domaine du droit civil que , dans la pratique , la violation du secret des correspondances pose les questions les plus délicates[151] Cela tient d'abord au fait que la jurisprudence rattache le principe de l'inviolabilité du secret à la théorie des droits de la personnalité et lui assigne comme fondement la personne même dont il est destiné à assurer la protection[152]

La personne qui, sachant qu'elle n'y est pas autorisée, se maintient dans un système de traitement automatisé de données ». Cela semble parfaitement justifié : le statut d'administrateur réseau ne permet pas un espionnage généralisé des correspondances. L'administrateur réseau remplit une fonction particulière et abuse de cette fonction chaque fois qu'il la détourne à des fins personnelles. Il n'est pas alors dans une situation différente d'un tiers espion. Une telle interprétation paraît exagérée à certains mais elle se justifie par le fait que le législateur n'incrimine pas seulement l'introduction sans droit dans un système, mais aussi le fait de s'y maintenir. Or, en cas de détournement, les droits d'origine sont nécessairement perdus. Le maintien s'avère alors frauduleux[153], on pourrait le contester en relevant que le respect des correspondances implique alors une action plutôt qu'une abstention, voire qu'il fait assumer au réceptionnaire un rôle dans la distribution du courrier qui n'est pas le sien. Néanmoins, les termes de l'incrimination sont suffisamment généraux pour permettre cette interprétation[154]

Ce n'est donc pas l'extension du fait justificatif tiré du respect des droits de la défense qui est condamnée en l'espèce, ce sont ses conditions d'existence qui sont mises en doute[155].

Liste des sources et références:

[1] J. PRADEL "Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée",. Dalloz,1971, chron. XVIII, p.1 11.n°6

[2] M. le CARBONNIER « Droit civil »,. T.1. 8ème éd. 1969,n°71.

[3] R. LINDON « Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée »,. JCP.1970.I. doctrine, n°2357 .

[4] F. GALLOUEDEC-GENUYS et Herbert MAISL « le secret des fichiers »,. Préf. Bernard CHENOT.éd.CUJAS.1976.p.6-7.

[5] B. DOCQUIR « Le droit de la vie privée », préf. Yves POULLET. Groupe de Boeck 2008. P. 226.n°552

[6] M. BRIAT « La délinquance informatique : aspects de droit comparé ». Actes du VIII° congrès de l'Association française de droit pénal organisé du 28 au 30 novembre 1985 à l'université de Grenoble., Economica 1986.p. 272.

[7] Martine BRIAT « la délinquance informatique : aspects de droit comparé »., op.cit.,p. 273.

[8] Y. BISMUTH « Droit de l'informatique, éléments de droit à l'usage des informaticiens »,. Ed. Harmattan.1er oct.2014. p.234.n562.

[9] J. EYNARD, « Les données personnelles : quelle définition pour un régime de protection efficace ? »,.éd. Paris : Michalon. 2013. P. 195.

[10] F. TERRE, D. FENOUILLET, « Droit civil. Les personnes, Personnalité, Incapacité. Protection », GEMEED. 2012, n° 106, p. 115 « La vie privée peut être envisagée sous deux aspects différents selon qu'il s'agit de la protection de son secret ou de la reconnaissance de son existence ». V. également B. BEIGNIER, « La protection de la vie privée in Libertés et droits fondamentaux », sous la dir. de R. CABRILLAC, M.-A. FRISON-ROCHE, T. REVET, Dalloz, 15 éd. 2009, n° 316, p. 205, qui évoque l'évolution du droit au respect de la vie privée vers un droit « à l'indépendance », « à la différence »: il ne s'agirait plus seulement de prétendre vivre caché, mais de vivre différemment: P. KAYSER, « La protection de la vie privée par le droit, Protection du secret de la vie privée », Préf H. MAZEAUD, 3ème éd.. Economica, 1995, n° 182-1. p. 344: « La protection de la vie privée comporte deux aspects distincts qui sont complémentaires. Le premier est la protection du secret de la vie privée [...]. La protection de la vie privée comporte, d'autre part, la protection de sa liberté »; D. GUTMANN, « Le sentiment d'identité, Etude de droit des personnes et de la famille, Thèse. Préf. F. TERRE, L.G.D.J., 2000, t. 327, n° 247, p. 221: « Le droit au respect de la vie privée est entendu, dans le droit et la société d'aujourd'hui, comme un droit à deux facettes. [...]. Selon une conception stricte, il s'agit d'un droit de contrôle portant sur des informations personnelles ; selon une conception large, il constitue une véritable liberté »; S. ABRAVANEL-JOLLY, La protection du secret en droit des personnes et de la famille. Préf. L. MAYAUX, Defrénois, 2005, t. 10, n° 719, p. 204: « On est ainsi amené à conclure que la protection de la vie privée comporte deux aspects distincts qui sont complémentaires. Le premier est la protection du secret de la vie privée [...]. Le second est la protection de la liberté de la vie privée ». in Émilie LINGLIN « corps humain et assurances de personnes »,. Th.univ. Panthéon Assas. 2 juillet 2014.n°41.p. 47

[11] Ibid

[12] Ibid

[13] « voix, image et protection des données personnelles »,. Commission nationales de l'informatique et des libertés. éd. documentation française. P. 59.

[14] M. CUSSON et G.LOUIS « L'art de l'enquête criminelle, à la recherche de la vérité, de la sécurité et de la justice » préf. Jean Marc BLOCH.éd 2019 (Canada), 2020 en Europe. P.126 et s

[15] Article 20 de la loi 09-08 « Lorsqu'il apparaît à la Commission nationale, à l'examen de la déclaration qui lui est fournie, que le traitement envisagé présente des dangers manifestes pour le respect et la protection de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet, elle décide de soumettre ledit traitement au régime d'autorisation préalable».

[16] Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[17] « Droit des données personnelles »,. DALLOZ DÉCRYPTAGE. 2019. P. 143.

[18] « Droit des données personnelles », op.cit. P. 151

[19] Les dispositions des articles 447-1, 44-2 et 447-3 ont été ajoutées en vertu de l'article 5 de la loi n° 103-13, susvisée.

[20] Art 447-1 CP « une sanction d'emprisonnement de six mois à trois ans d'une amende de 2.000 à 20.000 dirhams, à quiconque procède, sciemment et par tout moyen, y compris les systèmes informatiques, à l'interception, à l'enregistrement, à la diffusion ou à la distribution de paroles ou d'informations émises dans un cadre privé ou confidentiel, sans le consentement de leurs auteurs ».

[21] « Droit des données personnelles »,. op.cit,. P.152

[22] Le Dahir n° 1-14-175 du 21 rejeb 1441 (16 mars 2020) portant publication de la Convention européenne n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, dont le but est de

[23] « Protection des données personnelles et sécurité nationale, quelles garanties juridiques dans l'utilisation du numérique , à la croisée des droits »,. Cor. O. De DAVID Beauregard- Berthier et A-T KARLSSON. P.79

[24] Noémie VERRON « le contrôle de l'utilisation des données biométriques au regard des droit au respect de la vie privée »,. Préf. Hubert ALCARAZ.l'harmattan 2017. P. 27

[25] « Droit des données personnelles »,.op.cit,. n°921. P. 156.

[26] Art 10 du Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

[27] « Droit des données personnelles »,.op.cit,. P. 156.n°921

[28] M. VIVANT, B. WARUSFEL, N. MALLET- POUJOL« Le LAMY droit, du numérique »,. éd. 2022. P.320.n°670.

[29] loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

[30] « Protection des données personnelles », op.cit,.P. 60.n°1955.

[31] B. DOCQUIR « Le droit de la vie privée »,op.cit. P. 112.n°204

[32] De la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel,

[33] « Protection des données personnelles »,op.cit. P.64

[34] la section II de la loi 09-08[34] traite la qualité des données et consentement préalable de la personne concernée et plus particulièrement l'article 3

[35] F. MATTATIA « RGPD et droit des données personnelles : enfin un manuel complet sur le nouveau cadre juridique issu du RGPD et de la loi informatique et libertés de 2018 »,op.cit. P.84.

[36] N. MALLET-POUJOL « La place de l'individu dans un monde d'informatique globalisé »., in conseil de l'Europe, conférence européenne sur « la protection des données »., Actes 19-20 novembre 2001, pp. 85 et s,. P. 93.

[37] Constitution du 1er juillet 2011

[38] Directive 95/46/CE, art. 18, §1; loi du 8 décembre 1992, art. 17, § 1"; al. 1. Le Dahir n° 1-14-175 du 21 rejeb 1441 (16 mars 2020) portant publication de la Convention européenne n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, n'a pas traité une telle considération.

[39] G29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE. In « protection des données personnelles », dossier pratique. Ed. Francis LEFEBVRE. 20 octobre 2018. P.65

[40] G. HAAS « Guide juridique sur la protection des données personnelles »,. Data Pro. Avril 2018.p.57

[41] Y. BISMUTH « Droit de l'informatique, éléments de droit à l'usage des informaticiens »,. éd. Harmattan.1 er oct.2014.n°535. p.218

[42] M -L. DREYFUSS « La révolution digitale dans l'assurance : big data, RGPD, objets connectés, blockchain, assurtech », op.cit. P.184.

[43] CNIL, 19° Rapport d'activité, p.39.

[44] Art 4 loi 09-08 relative à la protection des personnes par le droit des données à caractère personnel

[45] A. DEBET, J.MASSOT et N. METALLINOS « Informatique et libertés : la protection des données à caractère personnel en droit français et européen »,. Coll. A. DANIS-FATÔME et O. LESOBRE.éd. Lextenso 2015. P.323,n°697.

[46] M-A. FRISON-ROCHE, « Penser le monde à partir de la notion de "donnée" »,.in M-A. ROCHE (dir), « internet, espace d'interrégulation »,.Paris, Dalloz, 2016,p.8

[47] V. SUZANNE, « L'effectivité de la protection des personnes par le droit des données à caractère personnel »,. Bruxelles, éd.Bruylant,2022. P. 218.n°263.

[48] J. FRAYSSINET, « Informatique, fichiers et libertés »,. Litec, 1992,n°172

[49] J. Frayssinet, op.cit.n°168 « Le danger pour les droit et libertés des individus dépend essentiellement de la finalité de l'utilisation des données nominatives et de celles des traitements automatisés »

[50] R. Gassin, Rép. pén. Dalloz, « Informatique et libertés », 1987, n°336

[51] M-H. BOULANGER, C. de TERWANGNE, Th. LÉONARD, Y. POULLET, S. LOUVEAUX et D. MOREAU « la protection des données à caractère personnel en droit communautaire »,. J.T.D.E. SEP. 1997.N°41. 5ème année. éd. LARCIER.

[52] Y. BISMUTH « Droit de l'informatique, éléments de droit à l'usage des informaticiens »,.op.cit,. p.218.n 535.

[53] P. SALVAGE « le consentement en droit pénal »,. RSC. 1991. pp. 699 et s

[54] J. LE CLAINCHE, « Consentement et traitement de données à caractère personnel », préc, sp p. 138; v. aussi plus généralement P. SALVAGE, Le consentement en droit pénal », préc.

[55] « Informatique et le droit pénal »,. P. CATALÀ .Trv. inst. Sc .crim. Poitiers. vol.I V. éd. CUJAS. 15 nov.1980. p.4

[56] T. LEONARD. et Y. POULLET., « La protection des données à caractère personnel en pleine (r)évolution», J.T., 1999, n° 52, note 144.

[57] « Informatique et le droit pénal »,. Ph. ROBERT, Trav.inst.sc.crim.Poitiers.vol.IV. éd. CUJAS. 15 nov.1980. p. 127.

[58] G. VILON- GUEZO « L'enquête pénale numérique à l'épreuve des nouvelles technologies » « données et technologies numériques » ., in « approche juridique, scientifique et éthique »., éd. Marie & Martin. Dir. N. NEVEJANS. P.234-235.

[59] P. KAYSER « la protection de la vie privée : protection du secret de la vie »,. Préf. Henri MAZEAUD. éd. ECONOMICA. . T. I. 1984 P. 469.n°279.

[60] Ed. GRAD « Inviolabilité du domicile ».th.univ. Paris. 1905. P.23

[61] Article 607-3 du code pénal

[62] Loi 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés.

[63] Loi 4 janvier 1980 relative à l'automatisation du casier judiciaire.

[64] A. BENSOUSSAN « informatique, télécoms,internet : réglementation, contrats, fiscalité, assurance, santé, fraude, communications électroniques, intelligence artificielle et robotique »,.op.cit. P. 10:30.°50:30.

[65]CA, 11 ch 5 avr. 1994, JCP E 1995, I, n° 461, obs VIVANT et Le STANC, LPA 1995, n° 80, p. 13, obs. Alvarez.

[66] CA, 3 ch. 21 janv. 1999, Juris-Data, n° 1999-040054

[67] « Commission dirigée par MM. Hérissé et Pintrand, avocats à la Cour ». Gaz. Pal. du 24 mars 1973, n° 82-83.

[68] P. KAYSER « La protection de la vie privée : protection du secret de la vie »,.op.cit. P. 491.n°289-1.

[69] Art 27 constitution Maroc.

[70] P. KAYSER « la protection de la vie privée : protection du secret de la vie »,. op.cit,.P. 106.n°86.

[71] P. KAYSER « La protection de la vie privée : protection du secret de la vie »,. op.cit, P. 102.n°84.

[72] J. PRADEL « Les dispositions de la loi du 17 juillet 1970 sur la protection de la vie privée »,.op.cit, p.114 n°23

[73] Art 447-1 du code pénal « Un emprisonnement de six mois à trois ans d'une amende de 2.000 à 20.000 dirhams à quiconque qui procède à l'interception, à l'enregistrement, à la diffusion ou à la distribution de paroles ou d'informations émises dans un cadre privé ou confidentiel, sans le consentement de leurs auteurs »

[74] I. LOLIES « La protection pénale de la vie privée »,. Préf. R. GASSIN.éd. presse-universitaires d'AIX-MARSEILLE-PUAM.1999.n°69.p.73.

[75] Albert CHAVANNE « Les atteintes à l'intimité de la vie privée au sens de l'article 368 du code pénal »,. In le droit criminel face aux technologies nouvelles de la communication ».op.cit,.p. 27

[76] A. BERTRAND « Droit à la vie privée et droit à l'image »,. Préf. X. LINANT DE BELLEFONDS. éd. Litec 1999.n°.274 et s. p. 130 et s

[77] I. LOLIES « La protection pénal de la vie privée »,.op.cit,.n°70.p.73 et s

[78] A. CHAVANNE « La protection de la vie privée dans la loi du 17 juillet 1970 ». Rev. Sc.crim.dr.pén.p.611

[79] R. PINTO « La liberté d'information et d'opinion en droit international » ECONOMICA 1984. P.104

[80] X. AGOSTINELLI « Le droit à l'information face à la protection civile de la vie privée »,. Préf. Ch. DEBBASCH. Librairie de l'université.1994. p.111.n°175

[81] Ph. MALAURIE et L. AYNÈS, « Droit civil: Les personnes », Cujas 1992, p. 122

[82] J. JAVANA « La protection des personnes contre la réalisation et la publication de leur image »., préf. Pierre KAYSER. LGDJ. 1978.p. 32.n°14.

[83] G. LEVASSEUR, « Rapport aux Journées de Madrid de l'Association Henri Capitant, Travaux de l'Association Henri Capitant », T. XIII, p. 187

[84] J. JAVANA « La protection des personnes contre la réalisation et la publication de leur image »., préf. P KAYSER. LGDJ. 1978.p. 29. n°12.

[85] Crim. 9 oct. 1980

[86] Poitiers, 7 janv. 1960, et Trib. corr. Seine, 30 oct. 1964.

[87] Crim. cass. 9 octobre 1980, D. 1981.I. 334.

[88] J. FOLLIET « L'information moderne et le droit à l'information »., chr. Soc. Fr.1969.p.230.

[89] Selon le paragr. 100 c. pr. pén. allemand de 1877, modifié par les lois des 25 juin 1969 et 31 mai 1978,

[90] Crim.cass. 9 octobre 1980, D. 1981.I. 334.

[91] J. MALHERBE « la vie privée et droit moderne »., préf. P. Antoine PERROD. éd. Comment faire. Légi. Jurisp. doct. p.88.

[92] « Quiconque par fraude ou à l'aide de menaces ou de violences contre les personnes ou les choses s'introduit ou tente de s'introduire dans le domicile d'autrui est puni de l'emprisonnement d'un à six mois et d'une amende de 200 à 250 dirhams. Si la violation du domicile a été commise soit la nuit, soit à l'aide d'une escalade ou d'effraction, soit par plusieurs personnes, soit

avec port d'arme apparente ou cachée par l'un ou plusieurs des auteurs, l'emprisonnement est de six mois à trois ans et l'amende de 200 à 500 dirhams ».

[93] R. LE BOURDELLES, « De l'inviolabilité de la personne et du domicile en droit français et comparé »,. Th.univ. RENNES. 1924. P.1

[94] R. LE BOURDELLES. op.cit,.P. 56

[95] R. LE BOURDELLES, op.cit,. P. 50

[96] B. FIORINI « L'enquête pénale privée : étude comparée des droits français et américains », éd.LGDJ. 4ème trimestre. 2018,n°146. p.103

[97] - Intitulé de section modifié et complété par l'article premier du dahir portant loi n° 1-74- 232 du 28 rebia II 1394 (21 mai 1974) modifiant et complétant la section IV du chapitre VII et le chapitre IX du titre premier du livre III du code pénal, Bulletin Officiel n° 3214 du 14 joumada I 1394 (5 juin 1974), p. 927.

[98] I. LOLIES « La protection pénale de la vie privée »,. op.cit.n°223.p.166.

[99] P.CASSAGNE « La notion du domicile et ses effets principaux en droit pénal »., th.univ. NANCY. 1937. P. 221.

[100] M. VÉRON « Droit pénal spécial »., 17ème éd. D. 2019. P. 244.n°360.

[101] Y. MAYAUD « Infractions contre les personnes : droit au logement et respect de la propriété d'autrui illustration associative d'une violation du domicile ».,op.cit. 264.

[102] Art 441 du code pénal « Quiconque par fraude ou à l'aide de menaces ou de violences contre les personnes ou les choses s'introduit ou tente de s'introduire dans le domicile d'autrui est puni de l'emprisonnement d'un à six mois et d'une amende de 200 à 250 dirham «

[103] Pierre CASSAGNE, op.cit. P. 221.

[104] M- D. FAUVEAU « Droit pénal spécial : livres 2 et 3 du code pénal : infractions contre les personnes et les biens 2010». Préf. Jacques Henri ROBERT. Collection. Essais. P.385.n°485.

[105] M-D .FAUVEAU « droit pénal spécial : livres 2 et 3 du code pénal : infractions contre les personnes et les biens 2010», op.cit. P.386.n°486.

[106] I. LOLIES « la protection pénal de la vie privée »,op.cit,.p.167, n°226

[107] P. BERALDI « La correspondance au point de vue de droit pénal »,. Th.univ. PARIS. 1906.p. 10

[108] J. PÉLISSIER « La protection du secret de la correspondance au regard du droit pénal »,. Rev sc.crim.et.dr.pén.comp., 1965,p.106

[109] J. PÉLISSIER « La protection du secret de la correspondance au regard du droit pénal »,. op.cit,.p.106

[110] Code pénal annoté, nouvelle édition par ROUSSELET, PATIN et M. ANCEL, t. 1, art. 187, n° 32; F. GOYET, Droit pénal spécial 8ème éd. par ROUSSELET, ARPAILLANGE et PATIN, n° 120; R. VOUIN, Droit pénal spécial, 5ème éd. par M.-L. RASSAT, nº 220, p. 286; A. DECOCQ, Rapport sur le secret de la vie privée en droit français, Le secret et le droit, Travaux de l'Association Henri Capitant, Journées libanaises, t. XXV, 1974, p. 474.

[111] « Droit de la donnée : principes théoriques et approche pratique »,. Préf. A. BILLIAU-LEPAGE, LexisNexis, Droit & professionnel communication et commerce électronique. P. 374n°1610.

[112] G. CARA-COSTEA « La correspondance privée »,. Th.univ. PARIS. 1908.p.9

[113] A. LEPAGE et H. MATSOPOULOU « droit pénal spécial »,. 1ère éd. THÉMIS. P.388 et s.n°555

[114] Ph. BONFILS, « Secret des correspondances »,. Rép. Pén. Dalloz.n°13

[115] Crim., 5 févr. 1958, J.C.P. 1958, II, 10580.

[116] Article 232 « Tout fonctionnaire public, tout agent du Gouvernement, tout employé ou préposé du service des postes qui ouvre, détourne ou supprime des lettres confiées à la poste ou qui en facilite l'ouverture, le détournement ou la suppression, est puni d'un emprisonnement de trois mois à cinq ans et d'une amende de 200 à 1.000 dirhams ».

[117] « Droit de la donnée : principes théoriques et approche pratique », op.cit. P. 374n°1610.

[118] Ph. BONFILS « Secret des correspondance », op.cit,.n°17

[119] CA Besançon, 5 janvier. 1978, II, 9449, note D. BÉCOURT

[120] A. LEPAGE et H. MATSOPOULOU « Droit pénal spécial »,. 1ère éd. Thémis. n°404, P.238.

[121] E. DREYER « Droit pénal spécial»,. LGDJ. 2020.p.238.n°404

[122] J. PRADEL. M.DANTI-JUAN « Droit pénal spécial : droit commun - droit des affaires»,. 8ème éd. CUJAS. 1er août 2020, p.203.n°219

[123] Ibid

[124] Emmanuel DREYER « Droit pénal spécial»,. LGDJ. 2020.p.236.n°400

[125].Ibid

[126] J. PÉLISSIER « La protection du secret de la correspondance au regard du droit pénal »,op.cit,.1965,p.107

[127] J.MALHERBE « La vie privée et le droit moderne », préf. P. Antoine PERROD. COMMENT FAIRE, coll ; E. BLANC. Janv 1968. P.16.

[128] M.QUÉMÉNER et J.P. PINTE « Cybersécurité des acteurs économiques : risques, réponses stratégiques et juridiques ».éd. LAVOISIER 2013.p.155 et s.

[129] Riom, 8 janvier 1849, D. 49.2.143.

[130] « Cass., 9 juin 1883, D. 84.1.89 »., 5

[131] Cass. crim. 15 mai 1990, Bull.crim.1990,n°196 ; Rev.sc.crim. 1991, p.572, obs. LEVASSEUR. « L'intention de nuire n'est pas au nombre des composantes du délit ».

[132] Ph. conte « Droit pénal spécial », op.cit., n°364.p. 267.

[133] CA. CHAMBÉRY 16 janvier 1961. Recueil DALLOZ de doctrine de jurisprudence et de législation de 1961 n°1. P.343

[134] « Jean MALHERBE « la vie privée et le droit moderne », préf. P. Antoine PERROD. COMMENT FAIRE, coll ; Emmanuel BLANC. Janv 1968. P.47.

[135] Chambéry 16 janvier 1961, D 1961-343 et la note, recueil général des lois 1961,I , n°279. P. 270

[136] E. DREYER « Abus de fonction d'un administrateur réseau : atteinte à un STAD et violation du secret des correspondances »,. Gaz. Pal. Jur. Mardi 18 juillet 2017.n°27. P. 2313

[137] E. DREYER « droit pénal spécial», op.cit.p.239.n°406.

[138] E. DREYER « Abus de fonction d'un administrateur réseau : atteinte à un STAD et violation du secret des correspondances »,op.cit,.n°27. P. 2313

[139] J. PRADEL. M.DANTI-JUAN « Droit pénal spécial : droit commun - droit des affaires»,. 8ème éd. CUJAS. 1er août 2020, p.203.n°219

[140] Ibid

[141] Emmanuel DREYER « Droit pénal spécial»,. LGDJ. 2020.p.236.n°400

[142].Ibid

[143] J. PÉLISSIER « La protection du secret de la correspondance au regard du droit pénal »,op.cit,.1965,p.107

[144] J.MALHERBE « La vie privée et le droit moderne », préf. P. Antoine PERROD. COMMENT FAIRE, coll ; E. BLANC. Janv 1968. P.16.

[145] M.QUÉMÉNER et J.P. PINTE « Cybersécurité des acteurs économiques : risques, réponses stratégiques et juridiques ».éd. LAVOISIER 2013.p.155 et s.

[146] Riom, 8 janvier 1849, D. 49.2.143.

[147] « Cass., 9 juin 1883, D. 84.1.89 »., 5

[148] Cass. crim. 15 mai 1990, Bull.crim.1990,n°196 ; Rev.sc.crim. 1991, p.572, obs. LEVASSEUR. « L'intention de nuire n'est pas au nombre des composantes du délit ».

[149] Ph. conte « Droit pénal spécial », op.cit., n°364.p. 267.

[150] CA. CHAMBÉRY 16 janvier 1961. Recueil DALLOZ de doctrine de jurisprudence et de législation de 1961 n°1. P.343

[151] « Jean MALHERBE « la vie privée et le droit moderne », préf. P. Antoine PERROD. COMMENT FAIRE, coll ; Emmanuel BLANC. Janv 1968. P.47.

[152] Chambéry 16 janvier 1961, D 1961-343 et la note, recueil général des lois 1961,I , n°279. P. 270

[153] E. DREYER « Abus de fonction d'un administrateur réseau : atteinte à un STAD et violation du secret des correspondances »,. Gaz. Pal. Jur. Mardi 18 juillet 2017.n°27. P. 2313

[154] E. DREYER « droit pénal spécial», op.cit.p.239.n°406.

[155] E. DREYER « Abus de fonction d'un administrateur réseau : atteinte à un STAD et violation du secret des correspondances »,op.cit,.n°27. P. 2313