Criminalité contemporaine en assurance terrestre

Droit pénal des assurances

الجريمة المعاصرة في التأمين على الأراضي

القانون الجنائي للتأمين

الباحث: السعيدي بشرى، دكتوراه في القانون الخاص، جامعة القاضي عياض، مراكش.

تاريخ الاستلام: ٢٠٢٤/٨/٩ تاريخ القبول: ٢٠٢٤ /٨/١٦ تاريخ النشر: ٢٠٢٤/٩/١٥

الملخص:

تحدث هذا المقال عن إن العالم الحقيقي والعالم الافتراضي ليسا منفصلين، ولكن البنية التحتية لتكنولوجيا المعلومات توفر الأدوات اللازمة للاتصال وتبادل السلع والخدمات. تعتمد المزيد والمزيد من المجالات، مثل التجارة أو حركة المرور على الطرق أو إمدادات الكهرباء أو التعليم، إلى حد كبير على تكنولوجيا المعلومات، ويمكن للهجوم السيبراني أن يضر بتوفير هذه الخدمات المادية، تتمثل الصعوبة الرئيسية التي تواجه أعمال التأمين في أن التطور الذي تتطلبه التكنولوجيات الجديدة والتصنيع يحفز حاملي وثائق التأمين على استخدام عمليات احتيالية جديدة بهدف تحقيق ربح غير مشروع.

الكلمات المفتاحية: الجريمة المعاصرة، التأمين على الأراضي، القانون الجنائي، للتأمين.

Abstract

Cet article parlait du fait que le monde réel et le monde virtuel ne sont pas séparés, mais que l'infrastructure informatique fournit les outils nécessaires pour communiquer et échanger des biens et des services. De plus en plus de domaines, comme le commerce, le trafic routier, l'approvisionnement en électricité ou l'éducation, dépendent dans une large mesure des technologies de l'information, et une cyberattaque peut nuire à la fourniture de ces services physiques. La principale difficulté à laquelle est confronté le secteur de l'assurance réside dans la sophistication. exigées par les nouvelles technologies La fabrication incite les assurés à recourir à de nouvelles opérations frauduleuses dans le but de réaliser un profit illicite.

Mots-clés : criminalité contemporaine, assurance foncière, droit pénal, assurance.

Introduction:

On peut donc supputer que l'éclosion d'une cyber civilisation qui repousse les frontières de notre espace habituel pose de nouveaux problèmes d'une acuité particulière puisque les actes délictueux sont perpétrés par des individus qui résident dans un pays différent de celui où sont portées les atteintes aux systèmes informatiques. On assiste à l'émergence d'une criminalité planétaire[1]. On peut plus particulièrement établir, dès lors, une liste exhaustive des différentes infractions modernes qui paraissent être les dernières venues dans le droit pénal des assurances. Les législations modernes mêmes ne semblent pas arriver à les distinguer. Cependant, le droit pénal contemporain n'est plus celui régissant, uniquement, les infractions ordinaires, mais parallèlement, il a une fonction de poursuivre le développement économique et industriel donnant naissance à des études de cas compliqués en comparaison avec ceux usuels.

La logique poursuivie place, alors, l'infraction du blanchiment de capitaux et le financement de terrorisme au sommet de l'ensemble des incriminations (I). Le législateur énumère une longue série d'infractions qui constituent des actes de terrorisme. Il est à préciser que les infractions visées sont toutes des infractions de droit commun, mais qui deviennent des actes de terrorisme lorsqu'elles sont commises « intentionnellement », dans un contexte terroriste[2]Surgit, ensuite, la fraude informatique d'acuité accrue (II)

I : Les fraudes financières : criminalité accrue en assurances

A- le blanchiment de capitaux

Il s'agit d'une opération qui consiste à masquer l'origine frauduleuse de sommes d'argent[3] C'est le fait soit de faciliter, par tout moyen, la justification mensongère des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect, soit le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit[4]. De sorte qu'elle ne peut avoir une seule forme juridique spéciale, le coupable du blanchiment apporte son aide à l'auteur de l'infraction d'origine. Si, en cela, il se rapproche du complice – chronologie mise à part – il se distingue du receleur, dont l'activité peut prendre une forme moins altruiste, lorsqu'il s'agit pour lui de bénéficier du produit de l'infraction d'origine[5]. [6]. Elle peut être, actuellement, retenue à l'encontre d'un individu qui procède au blanchiment du produit de sa propre infraction[7]Autrement dit, ces infractions de

---

[1] P. Arrigo, « La cybercriminalité : vers une régulation internationale de l'Internet ? », Gaz. Pal. 16 oct. 2001, n°289. p. 35

[2] Ph. BONFILS, L.GRÉGOIRE, « Droit pénal spécial », 25 janv. 2022, LGDJ. n°940.

[3] V. MALABAT « Droit pénal spécial », 9ème éd. Dalloz, 2020. P.557.n°883.

[4] H. ROBERT, « Réflexion sur la nature de l'infraction de blanchiment d'argent », JCPG 2008, 1 146, P. NÉRAC., «La répression de l'infraction générale de blanchiment », AJ pénal 2006, p. 440; M. SEGONDS, « Les métamorphoses de l'infraction de blanchiment... ou les enjeux probatoires de la lutte contre le blanchiment », AJ pénal 2016, p. 168.

[5] J. LARGUIER et Ph. CONTE « Droit pénal des affaires »,. éd. Paris : A. Colin 10ème 2010.p.241,n°257.

[6] J. LARGUIER et Ph. CONTE « Droit pénal des affaires »,. éd. Paris : A. Colin 10ème 2010.p.241,n°257.

[7] V.Cass. Crim. 25 juin 2003: JCP 2004, 1. 157. Dt. Pénal 2003. Comm. 142, obs. M. VÉRON; RSC 2004, p. 350, obs OTTENHOF : Gaz. Pal. 2004, Doctr. p. 790, obs DUCOULOUX-FAVARD pour l'arrêt de principe: Cass. Crim. 14 janvier 2004. Bull. Crim. n°12: JCP G 2004, II, 10081, note H. MATSOPOULOU : D. 2004, p. 1377, note Ch. CUTAJAR: Gaz. Pal. 17 avril 2004, p. 5, obs. O. RAYNAUD plus récemment: Cass Crim. 20 février 2008; Bull. Crim. n°43; Dr. Pénal 2008, Comm. 67, obs M. VÉRON; JCP G 2008, I, 146, note J.-H. ROBERT; JCP G 2008, II, 10103, note J. LASSERRE CAPDEVILLE; D. 2008, p. 1585, note Ch. CUTAJAR; AJP 2008, p. 234, obs. A. DARSONVILLE: D. 2009, p. 123, obs. T. Garé; RPDP 2008, p. 402, note V. Malabat.

conséquences établissent une distinction entre les régimes juridiques de deux infractions pourtant rattachées à la même catégorie et sur des points dont on estimait, jusqu'à maintenant, qu'ils devaient emporter une solution uniforme dans la catégorie[8]. Telle exprimée par D. CHILSTEIN « *une figure mal connue du droit pénal et dont la théorie générale, à supposer qu'elle soit possible, reste encore à établir* ». Composé des menaces[9] et vulnérabilité[10], le risque dans le cadre de lutte contre le blanchiment de capitaux révèle, d'une part, sur le plan national, des intimidations qui mettent en péril l'intégrité du système financier marocain. D'autre part, au niveau des entreprises ou des intermédiaires d'assurance, des abus qui pourraient être utilisés afin d'exécuter les actes incriminés.

a- Le fondement juridique du blanchiment des capitaux en assurance

Considérant le développement technologique et l'ouverture sur les marchés étrangers, les opérations peuvent être effectuées à travers de multiples moyens de communication et ce, sans avoir besoin de se déplacer auprès de la personne assujettie. Ces méthodes peuvent présenter un risque élevé de blanchiment de capitaux[11]. Divers pays s'attachent à instaurer des lois répressives afin de lutter contre le blanchiment de capitaux.

D'ailleurs, le champ d'application de l'infraction de blanchiment, dans la législation belge, a été conçu de façon fort large, puisqu'il englobe les avantages patrimoniaux tirés de toutes les infractions, quelle que soient leur nature ou leur gravité (crimes, délits et contraventions, infractions intentionnelles et non intentionnelles) et peu importe qu'elles soient prévues par le code pénal ou par les lois particulières[12.] Tandis que, la loi répressive italienne prévoit une double incrimination, une relative au blanchiment (*riciclaggio*) et l'autre à la réutilisation (*impiego*) de biens d'origine illicite. Qui sont de nature à couvrir toutes les étapes considérées par les études sociologiques et d'économie criminelle[13], comme étant constitutives du phénomène du blanchiment : depuis l'introduction des biens « illicites » dans les circuits financiers légaux (« emplacement ») à la dissimulation de l'origine criminelle par un ou plusieurs transferts successifs (« *layering* »), jusqu'à l'intégration définitive dans le circuit légal en tant que capitaux « blanchis », illicites et réutilisables[14.]

[8] A-M. LARGUIER « Immunités et impunités découlant pour l'auteur d'une infraction d'une infraction antérieurement commise par celui-ci » JCP 1961, 1, 1601

[9] les menaces c'est l'objet (ou la personne, ou l'évènement) qui peut causer un dommage (un impact négatif).

[10] Eléments internes au sein de l'entreprise (son dispositif plus explicitement) qui pourraient être exploités par la menace identifiée

[11] Art 12 al 1 Circulaire du président de l'Autorité de contrôle des assurances et de la prévoyance sociale n° AS/02/19 du 25 septembre 2019 relative aux obligations de vigilance et de veille interne incombant aux entreprises d'assurances et de réassurance et aux intermédiaires en matière d'assurances et de réassurance. B.O. n°6848 – 20 joumada I 1441 (16-1-2020).

[12] G. DELRUE, op.cit., p. 147.

[13] Surtout les études du GAFI. Pour tous, voy,. D. MASCIANDARO, E. TAKATS et B. UNGER, « Black finance ». in M-L. CESONI, Damien Vandermeersch, Ursula Cassani, Georgios Pavlidis, Geneviève Giudicelli-Delage, Aurélie Binet-Grosclaude, Juliette Tricot et Alberto di Martino « la lutte contre le blanchiment en droit Belge, Suisse, Français, Italien et international : incrimination et confiscation, prévention, entraide judiciaire », sous la direction, Maria Luisa CESONI. Bruylant avril 2013.p. 426 et s.

[14] S. MULINARI, Cyber Laundering, Milan, Pearson, 2003, notamment les chapitres 1 et 3-5. In Maria Luisa Cesoni, Damien, op.cit,p. 427 et s.

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

Quant au droit suisse, le dispositif de lutte contre le blanchiment d'argent fut complété par l'entrée en vigueur, le 1er avril 1998, de la loi sur le blanchiment d'argent (LBA) du 10 octobre 1997[15], qui définit les devoirs de diligence incombant aux intermédiaires financiers dans la lutte contre le blanchiment et aménage le contrôle administratif de ces professions[16].

On doit, notamment, rappeler ici que la convention de Vienne du 20 décembre 1988[17] contre le trafic illicite de stupéfiants et de substances psychotropes prévoyait pour les États membres l'obligation d'instituer un délit de blanchiment. L'adoption de mesures de confiscation des produits tirés des infractions de base et la création d'un groupe d'études, le groupe d'action financière internationale (GAFI)[18]. Les normes du GAFI constituent le socle de références et standards internationaux en matière de LBC/FT que les pays devraient mettre en œuvre au moyen de mesures adaptées à leur situation particulière[19]. En effet, les actes décrits par l'article 574-1 du code pénal ne sont répréhensibles en tant que tels, mais ils deviennent punissables dès lors qu'ils portent sur des avoirs provenant d'une infraction préalable[20]. L'incrimination ici étudiée se présente sous diverses variantes prévues par la loi pénale, visées respectivement aux 1°, 2°,3° et 4° de l'alinéa 1er de l'article 574-1[21], il s'agit d'une série d'activités d'acquis, de détention, d'utilisation, de conversion ou de transfert des biens d'infraction pénale. Elle requiert non seulement la dissimulation ou le déguisement de l'origine de ces biens, dans l'intérêt de l'auteur ou d'autrui, mais aussi l'aide d'une personne impliquée dans la commission de l'une des infractions préalables, ou de faciliter, par tous moyens, la justification mensongère de l'origine des biens ou des produits de l'auteur. ou, encore, l'apport d'un concours ou le don des conseils à une opération de garde de placement, de dissimulation, de conversion, de transfert ou de transport du produit direct ou indirect. L'alinéa 1er de l'article 574-1-5° prévoit le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des produits de l'auteur ayant procuré à celui-ci un profit direct ou indirect; Intervenant postérieurement à la commission d'une infraction. L'infraction est formelle dans la mesure où l'élément matériel se situe dans le simple fait de faciliter la justification mensongère de l'origine des biens et non dans la justification elle-même[22], il suffit d'avoir facilité la justification (par de fausses attestations, des déclarations

[15] ibid
[16] ibid
[17] La Convention a été adoptée par la Conférence des Nations Unies pour l'Adoption d'une Convention contre le Trafic illicite de stupéfiants et de substances psychotropes à sa 6ème réunion plénière, tenue à Vienne du 25 novembre au 20 décembre 1988. La Conférence avait été convoquée conformément à la résolution 1988/8 du 25 mai 1988 du Conseil économique et social, sur la base des résolutions 39/141 du 14 décembre 1984 et 42/111 du 7 décembre 1987 de l'Assemblée générale. La Convention est ouverte à la signature à l'Office des Nations Unies à Vienne, du 20 décembre 1988 au 28 février 1989, et ensuite au Siège de l'Organisation des Nations Unies à New York, jusqu'au 20 décembre 1989. signée par le Maroc 28 décembre 1988. Ratifiée le 28 oct 1992.
[18] A. LEPAGE et H. MATSOPOULOU « Droit pénal spécial », Thémis Droit. 1ère éd.2015. p.644. n°909.
[19] ACAPS « lutte contre le blanchiment de capitaux et le financement du terrorisme dans le secteur des assurances :Implémentation d'une approche basée sur les risques dans le cadre de la LBC/FC en assurance vie »., guide n°2. Décembre 2020.p. 11 et s.
[20] J. SPREUTELS et P. De MÛELENAERE (dir), « la cellule de traitement des informations financières et la prévention du blanchiment des capitaux en Belgique et dans le monde », actes du colloque international du 14 mars 2003, Bruxelles, Bruylant, 2003. p.29
[21] Institué en vertu de la loi n°43-05 promulguée par le dahir n°1-07-79 du 17/04/2007.
[22] V.MALABAT « Droit pénal spécial », éd. Dalloz. coll. « Hypercours »,6ème éd. 2013.n°831.

mensongères, des faux bulletins de salaire ou des fausses factures par exemple) et non d'avoir justifié l'origine des biens ou des revenus[23].

Le régime de la répression de l'infraction du blanchiment des capitaux est, généralement, indépendant de celui de l'infraction principale. La nature du délit principal impacte peu à l'égard de la répression de l'infraction de conséquence , « l'infraction principale peut bien avoir été réalisée à l'étranger, il n'en résulte pas une implication plus poussée de celle-ci dans le régime de l'infraction conditionnée qui conserve son autonomie dans la répression »[24]. L'influence de la prescription ou de l'amnistie de l'infraction principale par la loi étrangère est nulle[25]. La répression générale de l'infraction, du blanchiment de capitaux au Maroc, a été instituée, d'abord, par la loi 43-05[26]. En outre de la Circulaire du président de l'ACAPS n° AS/02/19 du 25 septembre 2019 qui apportent au paysage législatif demeurant en la matière, une panoplie de nouveautés ainsi que de précisions et des restrictions afin d'instaurer une parfaite compréhension aux entreprises d'assurances et de réassurance et à leurs intermédiaires, non seulement du dispositif, leur incombent des obligations de vigilance simplifiée et renforcée, mais encore d'une approche basée sur les risques dans la mesure d'une indispensable interaction entre les deux entités, les procédures de contrôle interne des organismes assujettis.

b- Taxinomie des cas de figures soupçonnés par les intermédiaires d'assurance

L'ACAPS a établi une panoplie de cas de figure de l'infraction de blanchiment de capitaux afin d'élucider les compagnies d'assurances de différents agissements frauduleux, principalement en assurance vie, employés par les assurés, pour prendre les mesures préventives nécessaires.

Une déclaration de soupçon faite par un intermédiaire d'assurance après un suivi minutieux des opérations effectuées à l'encontre d'un agent de commerce de n'avoir déclaré aucun bien immobilier et qui a souscrit un contrat d'assurance vie au mois de juillet 2020, il a opéré des cumules de versements de 1.000.000 MAD, d'au moins d'un an il a procédé au rachat du contrat d'assurance vie, rachetant ainsi une seconde résidence valant de 950.000 MAD, sans être soucieux de différentes pénalités encourues , alors que son revenu annuel ne dépassant pas 100.000MAD. Ces attendus ont obligé ledit intermédiaire à procéder à une déclaration de soupçon telle exigée par l'autorité de contrôle. Se fondant sur l'excès de versement en espèce ainsi qu'en chèque, l'ambiguïté des activités effectivement exercées par ledit commerçant, son

[23] M. DAURY-FAUVEAU « Droit pénal spécial : livres 2 et 3 du code pénal : infractions contre les personnes et les biens 2010 »,. Préf. J -H. ROBER . éd.PUF.p.131.n°130

[24] P. CAZALBOU « étude de la catégorie des infractions de conséquences : contribution à une théorie des infractions conditionnées »,. LGDJ. 2016, n°599, p.265

[25] C. LOMBOIS, « Droit pénal international », Dalloz, 2 éd.1979, n°380, estime que les normes d'amnistie et de prescription sont des formes d'abdication de sa compétence par un État, qui ne saurait donc renoncer à ce dont il ne dispose pas: la compétence que se reconnaît un autre État. On sait par ailleurs que la jurisprudence est indifférente à l'amnistie par un État étranger d'une infraction qui ressort à la compétence universelle française: V. Cass Crim. 23 octobre 2002; Bull. Crim. 2002, n°195 RSC 2003, p. 425, note M. MASSE: Rev. crim. DIP 2003, p. 309, note H. MATSOPOULOU ; D. 2004, p. 309, note M.-H. GOZZI. V. sur ce dernier point: L. DESESSARD, « Le recul de l'amnistie, in La pénalisation des responsabilité politiques en droit interne et en droit international », Travaux de l'institut de sciences criminelles de Poitiers, vol. n°26, Cujas, 2008, p. 125, spéc. p. 135.

[26] La loi 43-05 promulguée par le Dahir n° 1.07.79 du 28 rabii I 1428 (17 avril 2007), telle qu'elle a été modifiée et complétée par la loi n° 13-10, promulguée par le Dahir n° 1.11.02 du 15 safar 1432 (20 janvier 2011), dont le dispositif a été introduit aux articles 574-1 à 574-7 du code pénal principalement la section IV (bis) du chapitre IX qui traite « les crimes et délits contre les biens ». ainsi que le dahir n° 1-21-56 du 27 chaoual 1442 (8 juin 2021) portant promulgation de la loi n° 12-18 modifiant et complétant le Code pénal et la loi n° 43-05 relative à la lutte contre le blanchiment de capitaux.

insouciance nonobstant l'excessif montant des pénalités, le court délai entre la souscription et l'opération de rachat.

Consécutivement aux investigations menées, diverses infractions, escroquerie et contrebande, ont été confirmées par la cellule de renseignement financier à l'encontre dudit commerçant[27]. Les menaces pourraient être incarnées par des criminels, des facilitateurs, des groupes terroristes, ou bien des infractions sous-jacentes répandues sur le territoire national et dont le produit généré pourrait être investi dans des opérations de blanchiment de capitaux, quant à la vulnérabilité, il s'agit d'éléments internes au sein de l'entreprise (son dispositif plus explicitement) qui pourraient être exploités par la menace identifiée. La vulnérabilité des assureurs pourrait transposer par exemple une absence de KYC[28], ou d'un suivi faible des opérations[29].

Quelle que soit sa nature, délictuelle ou criminelle, l'infraction du blanchiment exige la mauvaise foi des circonstances de faits c'est-à-dire le caractère inhabituel de l'opération frauduleuse. L'article 133 du code pénal énonce d'une généralité extensive de l'élément intentionnel, « Les crimes et les délits ne sont punissables que lorsqu'ils ont été commis intentionnellement ». L'infraction de blanchiment suppose l'élément intentionnel qui ne peut être exclu que par l'intervention légale de la loi. Il faut donc que son auteur connaisse l'existence de l'infraction d'origine et qu'il sache que l'opération à laquelle il apporte son concours porte sur le produit direct ou indirect de celle-ci[30].

L'élément intentionnel ne pourrait exister sans le concours de la preuve qui atteste l'infraction, et qui ne sera, régulièrement, d'un apport facile, la connaissance de l'origine frauduleuse des biens blanchis s'induit des constatations de fait appréciées souverainement par les juges du fond au vu des éléments de preuve et des faisceaux de présomptions de faits soumis aux débats[31]. Mais il y a de fortes chances que la jurisprudence transpose les solutions rigoureuses dégagées pour le recel, en se montrant particulièrement sévère à l'égard des professionnels au point de consacrer de véritables présomptions de fait[32]

B- Le label terroriste

Insidieux comme le feu, le terrorisme jaillit spontanément là où l'on ne l'attend pas, couve sournoisement avant de se déclarer, se développe et se propage de manière irrationnelle, s'assoupit pour renaitre de ses cendres alors que chacun le croyait définitivement maîtrisé[33]

. Le terrorisme est une donnée isolée propre à certaines incriminations. Il est d'abord comme une condition préalable[34].La notion de « terrorisme » comme phénomène criminel, est très

---

[27] ACAPS « Typologies de blanchiment de capitaux et de financement du terrorisme dans le secteur des assurances »,. Document d'orientation Janvier 2022.p. 7

[28] Know Your Client (Connaître son client)

[29] ACAPS « lutte contre le blanchiment de capitaux et le financement du terrorisme dans le secteur des assurances :Implémentation d'une approche basée sur les risques dans le cadre de la LBC/FC en assurance vie »., guide n°2. Décembre 2020. P. 9 et s.

[30] J. LARGUIER et Ph. CONTE « Droit pénal des affaires »,. éd. Paris : A. Colin 10ème 2010.p.242,n°258

[31] Ch. CUTAJAR, « Blanchiment d'argent : prévention et répression »,.éd. Francis Lefebvre. 2018. p.101, n°205

[32] A. LEPAGE, P-M DU CHAMBON et Renaud SALOMON « Droit pénal des affaires ». 6ème éd. LexisNexis.2020. p.175.n°433.

[33] M- E. CARTIER « Le terrorisme dans le nouveau code pénal français »,. Rev.sc.crim.2. avr-juin.1995.p. 225

[34] Y. MAYAUD « terrorisme- infractions, poursuites pénales et indemnisation », Dalloz- Corpus. 2020. P. 24.n°2.

difficile à définir quant à son contenu[35]. Elle est juridiquement difficile à appréhender car c'est un phénomène mouvant et polymorphe[36]. Son appréhension pénale a été approuvée par la loi 03-03 du 28 mai 2003, créée dans le code pénal (a), particulièrement l'article 218. C'est, sans aucun doute, sous l'étendue des infractions nouvelles et particulières, que le législateur marocain a été, derechef, contraint de prévoir d'autres dispositions, afin d'asseoir la prévention ainsi que la répression de ladite infraction. En bonne logique, il a dû institué au sein du code pénal, en outre, la loi 13-10 du 20 janvier 2011, la loi 145-12 du 02 mai 2013, de même que la loi 86-14 du 20 mai 2015

For malheur, le code pénal marocain n'a procédé à aucune définition bien complète de la notion bâtie à chaux et à sable du terrorisme. Rigoureux vis-à-vis d'autres, il s'est contenté de dresser une liste des incriminations susceptibles d'être qualifiées de support. La notion juridique de terrorisme, alors, relève de deux critères, l'un emprunté à des comportements, dont la matérialité constitue l'assise de l'action terroriste, l'autre tiré de circonstances particulières, qui tiennent à une relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur et qui ont pour effet, de donner au comportement en cause leur dimension spécifique[37]. Cette condition devant être approuvée par des indicateurs de risque envisagés par l'ACAPS (b), pour pouvoir retenir la qualification de l'infraction[38]

a- Les agissements terroristes de support dans le code pénal et appliqués en assurance

L'amélioration de l'équilibre entre la répression et la protection des personnes impliquées dans un processus répressif, acquise au cours des trente dernières années, provient de l'extension des garanties accordées par le droit pénal, appliquées au droit quasi-pénal grâce à l'interprétation prétorienne de la notion de matière pénale[39]. Le législateur, restreint par une variété d'agissements terroristes, s'est dû institué des dispositions dans le code pénal pour répondre au degré de dangerosité des terroristes. Inopportunément le code des assurances n'était pas conjoint à ladite contribution. Toutefois, moins tranché qu'un dispositif octroyé par l'ACAPS rassemblant un assortiment de typologies de cas relatifs au blanchiment de capitaux et de financement de terrorisme dans le secteur des assurances vie et des assurances non vie afin de permettre aux intermédiaires ou aux entreprises d'assurances une déclaration de soupçon.

Quels sont donc les comportements interpolés en droit pénal et qui peuvent servir de base en droit des assurances ?

Une définition générale qui peut contribuer à identifier les principales caractéristiques des actes de violences usés par les terroristes incriminés par le code pénal et qui peuvent favoriser leur application en droit des assurances, il s'agit d'un « Ensemble des actes de violence (attentats

[35] A. SOTILLE « Le terrorisme international », Recueil des Cours, 1938, III, p. 95-96; P. MERTENS, « L'introuvable acte de terrorisme», dans: Réflexions sur la définition et la répression du terrorisme, Bruxelles, éd. U.L.B., 1974, p. 31 et s.; E. DAVID, « Le terrorisme en droit international (Définition, incrimination, répression) », in, Réflexions sur la définition et la répression du terrorisme, p. 109 et s.

[36] V.M.E cartier, op.cit, .p.12.

[37] Y. MAYAUD, op.cit, p. 27.n°. 9

[38] V. MALABAT, op.cit, p.599.n°.923.

[39] J. ALIX « Terrorisme et droit pénal : étude critique des incriminations terroristes»,. Préf. G. GIUDICELLI-DELAGE. éd. Dalloz. 2010. P.7,n°6

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

individuels ou collectifs, destructions...) qu'une organisation politique exécute pour impressionner la population et créer un climat d'insécurité »[40]. L'acte terroriste, lui, est un acte de violence isolé, sporadique, qui s'identifie à l'attentat, acte opéré par des individus seuls ou par quelques individus, dans la clandestinité, ayant pour but de faire entendre une cause, portant atteinte aux personnes et aux biens, par des moyens de violence tels que des explosifs. C'est ainsi que la jurisprudence, en France, définit l'attentat commis par des particuliers et l'identifie à l'acte terroriste[41]. Les articles de 218-1 à 218-4 du code pénal énumèrent un certain nombre d'infractions qui portent atteinte non seulement à la personne mais encore à des biens susceptibles d'être réunies à des fins terroristes.

Le premier critère de qualification, exigé par le législateur en vertu de l'article 218-1 al 1du code pénal, que les actes de terrorisme soient en relation avec une entreprise individuelle ou collective ayant pour but l'atteinte grave à l'ordre public par l'intimidation, la terreur ou la violence. Il s'agit de la volonté de vérifier l'existence « d' un dessein formé ou plan concerté se traduisant par des efforts coordonnés en vue de l'objectif à atteindre[42]. Il est, en effet, difficile de parler « d'entreprise » à propos d'un acte isolé, à moins d'en faire un synonyme d'action[43], une exigence d'entreprise individuelle ou collective est prévue par l'article 218-1 du code pénal « constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but l'atteinte grave à l'ordre public ». À savoir, une participation à une entreprise terroriste doit être établie tant au plan matériel que moral. Par conséquent, une anicroche se pose à cet effet relatif au lien de fidélité entre l'entreprise terroriste et l'acte accompli. Cette notion d' « entreprise » révèle le souci de pragmatisme du législateur, qui a cherché à appréhender le terrorisme à travers ses manifestations concrètes, c'est à travers ces dernières que l'entreprise, organisation destinée à préparer, promouvoir l'objectif poursuivi, apparaîtra[44]. La majorité de la doctrine estime que cette composante caractérise l'élément intentionnel et, en particulier, le « dol spécial[45] » ou le « mobile[46] » qui doit animer l'auteur de l'infraction. Une autre conception enseigne que ce « dol spécial » est constitué par deux éléments, l'un de nature objective, l'autre de nature subjective[47].

Au plan matériel, cela signifie que l'autorité de poursuites est en mesure de démontrer que l'infraction s'est inscrite dans un projet qui la dépasse. Elle a été l'un des moyens déployés pour atteindre une fin qui était de troubler gravement l'ordre public. Or, le contexte terroriste ne tient pas seulement à l'existence d'une entreprise objectivement établie et suffisamment prouvée[48]. Il exige, cependant, en outre de l'intention coupable prévue au titre de l'infraction qui lui est reprochée. L'auteur des faits aura l'intention de contribuer, par son acte, à une entreprise terroriste, dont la finalité est de troubler l'ordre public. Il s'agit d'une expression assez fréquente

---

[40] Dictionnaire de la langue française, le robert, 2ème éd. 1985,T9, p.258.

[41] P. SERRAND « Les notions juridiques d'attentat, d'attroupement et de rassemblement, en droit administratif de la responsabilité »,. Paris, LGDJ. 1994. Si le terrorisme est une notion législative, l'attentat est une notion jurisprudentielle. D. CUMIN « Tentative de définition du terrorisme à partir du *jus in bello* »,. Rev. sc. crim. doct. janvier 2004.p.18.

[42] A. CHALANDON, « séance du 7 août 1986, JORF, Débats parlementaires – Sénat », 8 août 1986, p. 4125

[43] Y. MAYAUD, op.cit. P.86.n°157

[44] B. CHEMIN et J-M HEBERT « la lutte contre le terrorisme »,. RSC, p.14

[45] M-E. CARTIER, op.cit.,p.233

[46] B. BOULOC « Le terrorisme », in problèmes actuels de science criminelle, vol.II, PUAM, 1989, p.70.

[47] A. LEPAGE et H. MATSOPOULOU, op.cit,. p.842.n°1170.

[48] Y. MAYAUD, op.cit,.p.87.n°

en matière pénale, notion vague, néanmoins, délimitée par le législateur qu'il l'a conservé, « désireux de distinguer les infractions terroristes d'autres agissements moins graves »[49].L'adverbe « intentionnellement » se servira à établir que le rapprochement de l'infraction commise avec une entreprise terroriste ne doit pas être accidentel ou fortuit. « Le ministère public doit donc démontrer la conscience qu'a eue l'agent participer à une entreprise ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur. S'il n'est pas nécessaire d'établir que son acte été directement accomplie dans ce but »[50]. L'infraction présente un caractère terroriste du fait d'un certain but (troubler gravement l'ordre public) et de certains moyens utilisés (intimidation ou terreur) et enfin de certaines données de fait (entreprise individuelle ou collective)[51]. La personne qui ferait, à son insu, quelque chose de normalement licite, qui serait utilisé par d'autres, dans un but terroriste, n'aurait aucun élément moral susceptible de qualifier une infraction quelconque et ne saurait donc, *a fortiori,* avoir le dol spécial nécessaire pour qualifier le terrorisme[52].

Du moment que l'élément moral doit s'analyser en rapport distinctement avec chacune de ses deux composantes : d'une part l'auteur du crime ou délit doit évidemment avoir eu l'intention requise par l'infraction « ordinaire » considérée, et d'autre part il doit avoir agir en sachant la relation de son acte avec l'entreprise terroriste[53], la finalité dudit acte n'est pas sollicité principalement, de l'auteur de l'acte, mais c'est essentiellement de l'entreprise toute entière, cela n'empêche pas qu'il le soit mais dans un groupe dont son mobile est bien caractérisé.

b- Les indicateurs de risques envisagés par l'Autorité de Contrôle des Assurance et de la Prévoyances Sociales (ACAPS)

La mutation du champ de la criminalité spéciale a contraint l'ACAPS d'instituer une approche générale des risques basée sur la collecte des indicateurs de base qui peuvent être appliqués par les intermédiaires et les entreprises d'assurance. Des critères de risques élevés à l'égard des assurés, aux opérations ainsi qu'aux contrats et produits commercialisés ont été institués afin d'incriminer les soupçons. L'autorité de contrôle des assurances s'accommode avec les différents intervenants dans l'opération d'assurances, elle procède à un voyage à l'univers des assurés : leurs catégories, leurs comportements, ainsi que d'autres critères supplémentaires.

Incontestablement, l'ACAPS vise une multitude de catégories de personnes qui suscitent un degré inévitable de risques. Quel est donc l'ordre apparemment bien intermittent qui préside ses catégories de clientèle ?

Il s'agit des catégories empruntées des recommandations du Groupe d'Action Financière (GAFI) pour une vigilance accrue, particulièrement au domaine de l'immobilier, à l'égard de toute personne physique ou morale contractant en assurance. En fait, les compagnies d'assurances

[49] M. RENARD, op.cit,. P. 258
[50] Cass. crim., 10 janv. 2017, B.n°14. Dr.pén.2017, n°35.Obs ph. CONTE
[51] J. LIMOUZY, « Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, sur le projet de loi relatif à la lutte contre le terrorisme et aux atteintes à la sûreté de l'État, Assemblée nationale », 1985-1986, n° 202, p. 6.
[52] Michel RASSAT, op.cit, n°859.p. 935.
[53] Ph. CONTE « Éléments constitutifs du crime de l'article 421-1 du code pénal »., juris-classeur. Dr pénal. Rev. LexisNexis. 2017.p.32

ont toujours été actives en accordant des emprunts hypothécaires à base d'assurances-vie[54]. Les intermédiaires et les sociétés d'assurances doivent être en mesure d'identifier les clients et les bénéficiaires effectifs, personnes physiques ou personnes morales, leurs activités commerciales, notamment, commercialisation des biens luxes, des perles et des bijoux, une PPE[55] ainsi que ses proches et sa famille qu'ils soient de nationalité marocaine ou étrangère résidents ou non qui simulent des indices de risques élevés[56]. Bien affirmé par l'ACAPS, la criminalité terroriste expose le domaine d'assurance aux pratiques idéologiques des groupes terroristes. Ces derniers ont souscrit, en escroquerie, avec un intermédiaire d'assurance diverses polices , afin de mettre en exergue leurs projets terroristes, portant atteinte à l'ordre public[57]. En outre, les organisations à but non lucratif et toutes constructions juridiques ainsi que tout rapport de droit par lequel des actifs sont transférés à une ou plusieurs personnes, à charge pour elle(s) de les gérer, de les utiliser, le cas échéant, et de les remettre selon le but défini par le constituant. Ce but peut être de nature générale ou en faveur des bénéficiaires[58] ce qui est désigné par « *trust* », et qui présenterait des risques d'utilisation illicite du fait de la confidentialité qui peut offrir[59].

Tenant d'une main la balance et de l'autre le glaive[60], l'autorité compétente retient l'indice, également, du comportement du client. Inexorablement les réactions inopinées des clients en dépits de leurs informations personnelles, ainsi que leur renonciations fortuites sans aucune sollicitude des intérêts effectifs vis-à-vis d'une demande d'intensification de confidentialité qui n'est guère réclamée par la multitude des autres assurés et qui engendre, singulièrement, la vigilance des intermédiaires ainsi que des sociétés d'assurances. d'ailleurs, le financement de terrorisme est chevronné par diverses opérations effectuées par ces intermédiaires d'assurances, requises par leurs clients, le recours à des opérations compliquées en proportion des autres habituellement effectuées. La complexité de la situation apparaît, particulièrement avec l'apparition de techniques et l'utilisation de services virtuels « est bien l'impossibilité de rencontrer physiquement la contrepartie avec laquelle il entre en relation d'affaires. Afin de maîtriser au mieux la dépersonnalisation de ces relations à distance et d'atténuer ainsi cette virtualité »[61]. En outre, la proportionnalité de risque est assez notable lorsque le bénéficiaire effectif résident dans un pays présentant un risque élevé de blanchiment de capitaux ou de

[54] Le remboursement des emprunts hypothécaires est aussi une technique de blanchiment employée et par laquelle les amortissements sont faits par des versements en liquide mensuels.G. DELRUE « Le blanchiment de capitaux et le financement du terrorisme »,.2ème éd. 2014.p.323.n°798.

[55] PPE: Personne Politiquement Exposée.

[56] « Lutte contre le blanchiment de capitaux et le financement du terrorisme dans le secteur des assurances »,. Guide n°2.implémentation d'une approche basée sur les risques dans le cadre de la LBC/FT en assurance vie.p.26

[57] ACAPS « Typologies de blanchiment de capitaux et de financement du terrorisme dans le secteur des assurances »,. Document d'orientation Janvier 2022.p. 15.

[58] C. DERGATCHEFF « Droit comparé en matière de mécanismes fiduciaires : pays anglo-saxons, Suisse, Luxembourg », JCP., n°36, 6 sept 2007, p.46

[59] B. GUILLAUME « Confidentialité et prévention de la criminalité financière : étude de droit comparé »,.éd. Bruylant.2017. p.260.n°548.

[60] Énonciation de J. ORTOLAN « Éléments de droit pénal : pénalité, juridictions, procédure, la science rationnelle, la législation positive et la jurisprudence avec les données de nos statistiques criminelles »,. éd. Plon (Paris), 2 vol. 1875

[61] B. GUILLAUME, op.cit,. p.260.n°548

financement du terrorisme, ou en relation avec ces pays, notamment les opérations classées comme telles par les instances internationales compétentes[62].

En vertu de La Circulaire de l'Autorité de Contrôle et de Prévoyance Sociale relative au devoir de vigilance qui exige aux assujetties, intermédiaires et compagnies d'assurances, de procéder à l'analyse, l'évaluation et l'interprétation, au moins une fois par an, des risques relatifs au financement du terrorisme. Il en résulte qu'un intermédiaire d'assurances a établi une vérification et une analyse des listes des clients sanctionnés dont il a conclu qu'un souscripteur, M.X ,est figuré au sein des multiples listes de sanctions. À cet égard, il a déclaré le soupçon constaté à la cellule compétente conformément aux restrictions envisagées.

Multiples facteurs qui se manifestent pour le financement du terrorisme, expressément le cas où les intermédiaires souscrivent des contrats dont les seuils dépassent ceux fixés par l'autorité compétente. Ce sont surtout ces produits financiers avec une prime unique ou des périodiques, sans avantage fiscal, qui forment un risque élevé[63]. M. CUTAJAR démêle : « la réduction de la menace terroriste l'affaiblissement des moyens terroristes et la communauté internationale considère le gel des avoirs comme un des moyens déterminant pour lutter non seulement contre le financement terrorisme mais également contre le terrorisme lui-même en dissuadant d'éventuels candidats à financer des activités terroristes, en révélant les circuits monétaires du financement du terrorisme qui peuvent fournir des indices sur des cellules terroristes et des financiers de terrorisme non encore identifiés, en permettant de saler des réseaux de financement du terrorisme, en encourageant des personnes visées à se désolidariser des activités terroristes et à renoncer à leur affiliation à des groupes terroristes [64]

II : La fraude informatique : le surcroît d'une criminalité en assurance

L'expression « fraude informatique » doit recouvrir un domaine limité pour avoir un sens juridique. Trop large, elle ne permet plus au juriste de saisir son contenu, ni d'isoler un lien avec l'infraction informatique. Le concept de fraude informatique pourrait se définir de lui-même si le juriste distinguait la fraude informatique, de la fraude au moyen ou à l'aide de l'informatique. Son étude permettrait d'exclure l'ensemble des infractions dont l'élément légal n'est pas directement en relation avec un système de traitement automatisé de données[65]

Diverses propositions doctrinales, de la fraude informatique[66], ont été maintenues afin de satisfaire le vide juridique imposé par le législateur, puisqu'aucune définition n'a été introduite

[62] « Lutte contre le blanchiment de capitaux et le financement du terrorisme dans le secteur des assurances »,. Guide n°2.implémentation d'une approche basée sur les risques dans le cadre de la LBC/FT en assurance vie.p.27

[63] G. DELRUE, op.cit,.p.324.n°799

[64] Ch. CTAJAR « Le gel des avoirs terroristes, nouvel outil de lutte contre le financement du terrorisme »,. JCP. G. Actualités. Aperçue rapide.17 mai 2006.p.214

[65] J-F. CASILE, « Le code pénal à l'épreuve de la délinquance informatique »,. Préf. G. FAURÉ, univ. D'Aix- Marseille. I.S.P.E.C. 2002. P.21.n°18.

[66] X.LINANT de BELLEFONDS, « L'informatique et le droit », PUF. Que-Sais-Je?, 1998; X. LINANT de BELLEFONDS et A.HOLLANDE, « Pratique du droit de informatique », Encyclopédie Delmas, 1998: J.DEVEZE « Les qualifications pénales applicables aux fraudes informatiques », in 18 Congrès AFDP, « le droit criminel face aux technologies modernes de la communication, Economica et ADT, 1986, p. 185; J. DEVEZE, « Commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique » Lamy Droit de l'Informatique, 1987, Bull. act J, fév. 1988, p. 3; J. DEVEZE, « La fraude informatique- Aspects juridiques», JCP., 1987, éd. G., n° 25, 1, 3289; J.DEVEZE, Droit pénal des affaires », JCP, 1988, éd. E n°7, 1, 15122; DEVEZE (J.), Le vol de biens informatiques, JCP., 1985, éd. G. 1, 3210; DEVEZE. Infractions en matière informatique, Juris Classeur pénal, Art. 462-2 à 462-9 commentaire, 1988; DEVEZE (1) Loi du 5 janvier 1988 relative à la

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

avec les dispositions légales de traitement automatisé de données. MM. ALTERMAN et BLOCH retiennent comme définition du délit informatique celle proposée par les experts de l'Organisation pour la Coopération et le Développement Économique (OCDE), à savoir « *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données* »[67]. Ces juristes, intégrant dans leur définition la notion de morale, semblent considérer que le droit pénal ne peut à lui seul contenir toute l'approche « sanction » de l'utilisation frauduleuse de l'informatique »[68].

L'objet de la fraude informatique est donc constitué par les données représentant des biens et introduites dans les systèmes de traitement de données (A). Dans la majorité des cas de fraude informatique, les biens représentés par les données sont des biens immatériels tels que de la monnaie scripturale, des créances…etc[69]. Ces éléments, en revanche, ne peuvent être constitutifs de l'infraction que si leur usage est frauduleux (B).

A- L'accès ou le maintien frauduleux d'un système de traitement automatisé des données en assurance

L'atteinte à un système de traitement automatisé de données, en assurance, comportant un dispositif de sécurité, traduit une démarche offensive de la part du délinquant, assuré comme assureur, qui n'est pas stoppé dans sa démarche malveillante et qui exprime, à travers la poursuite de son acte, un comportement dangereux. La violation d'un dispositif de sécurité révèle le franchissement d'une étape supplémentaire dans l'intention de porter atteinte au système. En ce sens, elle implique de considérer les conséquences de la violation du dispositif de sécurité qui permettent parfois de repérer les traces laissées par le délinquant, facilitant alors la connaissance de son identité ainsi que les poursuites, le jugement et la condamnation qui en découlent[70]. Quoi qu'en dise l'exposé des motifs, ce n'est plus l'accès lui-même qui est incriminé mais la main mise

---

fraude informatique, DIT, 1988, n° 1, p. 81: J. DEVEZE, «Droit et informatique: un mariage difficile », DIT, 1988, m2, p. 11; J. DEVEZE, « Infractions en matière informatique », Juris-Classeur pénal, Art. 462-2 et 462-9, 1988. R. GASSIN, « La protection pénale d'une nouvelle « universalité de fait » en droit français: les STAD- commentaire de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatiques, Act lég. Dalloz, 1989, p. 13; R.GASSIN, «La première application de la loi sur la fraude informatique», Lamy Droit de l'Informatique, 1989, Bull, actualité B, p.3: GASSIN (R.), Informatique (Fraude Informatique)», Rep. Dallaz, Droit pénal - Procédure pénale, oct 1995; R. GASSIN, « Informatique et libertés », Rep. Dalloz, Droit pénal- Procédure pénale, janv. 1987; R. GASSIN, Un cas exemplaire de dérive jurisprudentielle du droit pénal technique: l'arrêt de la Chambre crim. du 3 nov. 1987 relatif aux délits en matière d'informatique, de fichiers et de libertés », Lamy Droit de l'Informatique, 1988, Bull actualité n" B, p. 2; R. GASSIN, « Le droit pénal de l'informatique », D., 1986, Chron, p. 35;R. GASSIN, « Au sujet du délit d'atteinte volontaire aux données contenues dans un système de traitement automatisé de données (Commentaire d'un arrêt de la Chambre criminelle du 5 janvier 1994) », Lamy Droit de l'Informatique et des réseau, Bull. actualité B, mai 1996, n°81; CROZE (H.), «L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique) », JCP, 1988, éd. G., n° 18, 1, 3333; N. AUPECLE-GUICHENET , « Les infractions pénales favorisées par l'informatique », Thèse Montpellier, 1984: G. CHAMPY. « La fraude informatique », Presses Universitaires d'Aix-Marseille, 1992; A. FRYDLENDER, « La fraude informatique, étude phénoménologique et typologie appliquée au contexte français », Thèse Paris, 1985; S. JERRARI, « La fraude informatique », Thèse Montpellier, 1986.

[67] H. ALTERMAN et A. BLOCH, «La fraude informatique », Gaz. Palais, 3 sept. 1988, P. 530

[68] J-F. CASILE, « le code pénal à l'épreuve de la délinquance informatique »,. Préf. G. FAURÉ, univ. D'Aix- Marseille. I.S.P.E.C. 2002. P18, n°10

[69] U. SIEBER, « la délinquance informatique : les délits économiques liés à l'informatique et les atteintes à la vie privée »,. Précis et travaux. Fac. Dr. Namur. Trad. S. SCHAFF. Revue. M. BRIAT.1990. P.8

[70] J-F. CASILE, « le code pénal à l'épreuve de la délinquance informatique »,. Préf. G. FAURÉ, univ. D'Aix- Marseille. I.S.P.E.C. 2002. P. 448.n°1243.

sur le support de l'information[71]. Il importe donc d'envisager la conception du système de traitement de données concomitante au droit (a). La seule démarche acceptable consiste alors d'examiner les éléments constitutifs de l'infraction (b).

a- **La recherche de conceptualisation du système de traitement automatisé de données en droit.**

L'adaptabilité du droit, contraint à remettre en cause des représentations juridiques de base qui conduisent celui-ci à se pratiquer sans certitude[72]. De sorte que la révolution numérique bouscule l'ensemble des modèles économiques, technologiques et sociaux habituels. Mais elle modifie aussi profondément le rapport à la norme, qu'il s'agisse de sa substance, de son élaboration ou de son application. L'accompagnement de l'innovation, en assurance, implique en effet de passer d'une logique de réglementation et de garantie à une logique de régulation, c'est-à-dire à un type d'encadrement et d'accompagnement qui combine la fidélité à des principes fondamentaux et à une règle de droit claire, et des nouveaux modes d'intervention du régulateur, fondés sur le droit souple[73]. Le droit de l'informatique vient s'insérer dans des catégories intellectuelles connues mais qui, dans le même temps, vient, sinon les bouleverser, obliger à les remettre en cause[74].

En l'occurrence, la Convention de Budapest utilise le terme « système informatique », selon les auteurs de ce texte, ce système peut comprendre des moyens d'acquisition, de restitution et de stockage de données, il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau et sans intervention humaine directe. Les ordinateurs sont constitués d'un ensemble de ressources matérielles et logicielles, pour assurer la meilleure disponibilité de ces ressources, il faut une organisation de tout l'ensemble. Les systèmes ne sont autres que des super programmes chargés de cette organisation ; ils complètent en quelque sorte la logique de la machine. Le système d'exploitation (operating system) est le système qui permet d'exploiter et de gérer la machine. Il est constitué de plusieurs systèmes particuliers ayant chacun des attributions bien définies[75]. La mise sous tension d'un ordinateur génère une volonté de la part de l'utilisateur, d'activer, à partir du clavier ou de la souris, un programme. L'exécution d'un train de programmes fait appel à un système appelé moniteur[76]. Chaque programme du « train moniteur » comporte obligatoirement en tête, les instructions nécessaires, permettant au système de passer à l'exécution. Les systèmes appelés superviseurs ont pour but de gérer les ressources de la machine, ce sont par exemple, les superviseurs de chargement, d'entrées-sorties ou de surveillance de l'exécution[77]. Le système d'exploitation, lui, assure et contrôle l'exécution de tous les programmes

[71] J. DEVEZE, « La fraude informatique-Aspects juridiques », JCP., 1987, 1, 3289.n°18.
[72] M. VIVANT, « Sciences et praxis juridique », D., 1993, Chron., p. 109
[73] É. GEFFRAY, « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? »,. Les nouveaux Cahiers du Conseil constitutionnel, 1er juin 2016,n°52, p.7

[74] M. VIVANT « Le produit informatique, Discours sur un discours », D., 1989, Chron.,p. 140

[75] P. MATHELOT, « L'informatique, Que-sais-Je? », PUF, 1995, p. 34
[76] Le train moniteur représente une série de travaux présentés à l'ordinateur en séquence, un seul travail étant présent en machine à un instant donné. note, J.-F. CASILE, « le code pénal à l'épreuve de la délinquance informatique »,. Préf. G. FAURÉ, univ. D'Aix- Marseille. I.S.P.E.C. 2002. P. 69,n°158
[77] P. MATHELOT, « L'informatique, Que-sais-Je? », PUF, 1995, p. 35

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

exploitables de la machine. Il est situé dans la mémoire centrale lorsque l'ordinateur est sous tension[78].

L'opération de traitement est certainement l'opération centrale du processus de numérisation. Le traitement de l'information comprend la transformation, la transmission, la conservation d'informations, mais, surtout, leur combinaison et leur création. Une fois l'information recueillie, et éventuellement stockée, elle peut faire l'objet d'un traitement au sens de combinaison d'informations. Tout processus intellectuel est une opération de combinaison d'informations qui s'exécute exclusivement par la combinaison des sémantiques des informations données. Pour réaliser mécaniquement des combinaisons d'informations, il faut pouvoir combiner simultanément les supports et les sémantiques des informations. Cela implique qu'à un support correspond une seule sémantique : c'est ce qu'on appelle une information univoque. Seules les informations univoques sont mécanisables. La mécanisation de certaines fonctions mentales de l'homme, réalisées par un processus analogique, a permis la construction d'automates, puis de machines automatiques dans l'industrie (...) c'est ce qu'on appelle automation ou automatique, qui, combinée avec le mot information, a donné naissance au mot informatique, forgé par M. Philippe Dreyfus[79]. Cet auteur considère donc le traitement comme « l'ensemble des opérations de collecte, de transformation, de conservation, de transmission, de combinaison et de création de l'information.

L'approche doctrinale renvoie à l'interprétation de La notion de « connaissance » qui doit être comprise comme « le résultat de l'exercice de cette fonction de la vie psychique (la fonction de connaissance) qui se manifeste par des phénomènes ayant un caractère représentatif et objectif (*les savoirs*). Il s'agit d'un savoir sur un objet extérieur à la conscience qui se traduit par une idée de cet objet, c'est en somme une idée de quelque chose, une notion d'un objet de connaissance[80] La connaissance composerait donc l'information qui serait « le contenu informatif de la donnée »[81], laquelle serait employée au sens de donnée brute, c'est-à-dire non structurée. Le contenu informatif de la donnée désigne non seulement les éléments d'information qui sont traités par le système, mais aussi les représentations conventionnelles des éléments de programme qui servent à le traiter[82].

[78] La mémoire centrale se compose de la mémoire morte et de la mémoire vive. La mémoire morte ou ROM (Read Only Memory) ne fait que l'objet de lectures. La mémoire vive ou RAM (Random Access Memory) permet de stocker les programmes et les données utiles au fonctionnement de l'ordinateur. Le contenu de la mémoire vive s'efface lorsque l'ordinateur n'est plus sous tension., J-F. CASILE, « le code pénal à l'épreuve de la délinquance informatique », op.cit.p. 69,n°158.

[79] M. BUFFELAN précise que la définition du mot informatique, retenue le 6 avril 1967 par l'académie française qui la définie comme « la science du traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines, et des communications dans les domaines techniques, économiques et sociaux n'est pas satisfaisante car ambigüe. Il lui préfère la définition retenue par M. Jacques ARSAC à savoir « la science du traitement logique et automatique de l'information », in ARSAC (J.), « La Science informatique », Paris, Dunod, 1970, p. 50

[80] R. GASSIN, « Informatique : Fraude informatique », Rép. Pén, Dalloz, oct. 1995, nº 50

[81] J. DEVÈZE, op.cit., 1, 3289

[82] R. GASSIN, op. cit., n°53

b- La qualification de l'infraction au sens de l'article 607-3 du code pénal

L'infraction suppose que le détournement porte sur des données d'un traitement automatisé et non clandestin. Le caractère automatisé du traitement ressort des termes même de l'article 50 de la loi 09-08[83]. Un non-lieu a pu être prononcé dans une affaire dans laquelle il résultait de l'examen des pièces de la procédure que « *si une table de concordance informatisée avait bien été utilisée afin de retrouver le contrat litigieux, l'information nominative communiquée ne provenait pas de cette table mais du support papier du contrat d'assurance* »[84][85]. L'exigence d'absence de clandestinité du traitement est la conséquence du fait que la finalité d'un traitement est définie. Comme le rappelle le texte d'incrimination, par la disposition législative, l'acte réglementaire ou la décision de l'autorité compétente autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement. Or, l'absence du respect des formalités préalables à la mise en place d'un traitement fait obstacle à la détermination de la finalité du système[85], dans une telle hypothèse, des poursuites restent cependant possibles. Elles doivent alors être fondées sur l'article 51 de la loi 09-08[86] qui prévoit « Sans préjudice des sanctions pénales, lorsqu'il apparaît, à la suite de la mise en œuvre du traitement objet de la déclaration ou de l'autorisation prévue à l'article 12 de la présente loi, que ce traitement porte atteinte à la sûreté ou à l'ordre public ou est contraire à la morale et aux bonnes mœurs, la Commission nationale peut, sans délais, retirer, selon le cas, le récépissé de la déclaration ou l'autorisation, qui sanctionnent le non-respect des formalités préalables »[87], étant rappelé que les peines encourues sont identiques »[88].

L'article 462-4 ancien du Code pénal français, en concomitance l'article 607-6 du code pénal marocain[89], permettait d'incriminer l'atteinte au système, par le maître du système lui- même, lequel ne peut se rendre coupable du délit prévu à l'ancien article 462-2. L'auteur se référait donc à l'expression « d'abus d'autorisation d'accès à un système informatique »[90], en considérant que le texte ne faisant plus référence à la notion d'accès frauduleux, il y a lieu d'en déduire que ce délit

[83] Art 50 de la loi 09-08 dispose « La création, la tenue et le traitement de registres centraux concernant les personnes soupçonnées d'activités illicites, de délits et d'infractions administratives et les décisions prévoyant des peines, des mesures de sûreté, des amendes et des sanctions accessoires relèvent des seuls services publics qui ont une compétence expresse en vertu de la loi d'organisation et de fonctionnement et qui doivent respecter les règles de procédure et de protection des données prévues par la loi, après avis de la Commission nationale »

[84] Cass. crim., 14 mai 1996, n° 93-80.982.

[85] Dans l'hypothèse où les formalités préalables ne sont pas respectées, la CNIL dispose, depuis 2004, d'un pouvoir de sanction (L. n° 78-17, 6 janv. 1978, art. 45) et peut prononcer, entre autres, une injonction de cesser le traitement (hypothèse de la déclaration) ou un retrait de l' autorisation (hypothèse de la demande d'autorisation)..

[86] 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

[87] en ce sens, V. CA Rouen, 23 oct. 2014, n° 13/01431 : JurisData n° 2014- 031544

[88] A.MIHMAN, « Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » JCP. 1er janvier 2018. P. 12

[89] Art 607-6 C.P « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé des données ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient, leur mode de traitement ou de transmission, est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement ».

[90] J-P. BUFFELAN, op.cit., p.102

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

suppose, de la part de son auteur, un accès régulier. Le Professeur Gassin critique cette position en considérant qu'elle ignore le fait que l'article 323-2 du code pénal français, l'article 607-5 du Code pénal marocain, ne stipule pas davantage d'accès frauduleux et qu'à admettre le raisonnement de son auteur, il faudrait également étendre sa conception au délit d'atteintes volontaires au fonctionnement d'un système de traitement automatisé de données[91]. L'approche de MM. GASSIN et BUFFELAN, ne peut trouver de justification qu'après avoir précisé le sens du mot « entrave » qui, suivant un sens matériel ou logique, emporte deux significations différentes. Une entrave matérielle ne nécessite pas d'accès ou de maintien frauduleux, tandis que l'entrave logique nécessite d'accéder préalablement au système, pour que le délit soit constitué[92].

En outre, l'élément intentionnel devrait être en l'occurrence omniprésent, le comportement d'un individu est réprimé selon son intention[93]. L'intention se comprend, quant à la conception classique remise en cause, l'élément indispensable pour la qualification de l'infraction. Par conséquent, incriminer ne consiste pas seulement à définir un comportement matériel car une infraction est toujours la conséquence d'une action humaine et la réparation sociale qui s'attache à la lésion d'une valeur protégée varie selon l'état d'esprit dans lequel l'agent a agi. La confusion doctrinale proviendrait de ce que l'intention est une technique législative d'incrimination et que les auteurs qui tentent de la définir, se sont inspirés de la « théorie Judiciaire de la responsabilité pénale individuelle »[94]. C'est la condition d'imputation particulière à certaines incriminations, comme (...) la volonté de commettre le délit tel qu'il est déterminé par la loi, ou encore la conscience chez le coupable d'enfreindre les prohibitions pénales[95].

L'article 607-3 al 1C.P incrimine « Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ». L'élément intentionnel découle, ainsi, de l'adverbe « frauduleusement », lequel s'adresse aussi bien à l'accès qu'au maintien[96]. Le terme « frauduleux» suppose que l'intrusion et le maintien aient été volontaires et que leur auteur ait eu conscience de commettre une action illicite[97]. Un accès accidentel n'est pas puni; l'infraction n'exige, par contre, pas de volonté de nuire ou d'intention de lucre[98]. Parfois, le caractère frauduleux est évident. Ainsi par exemple, un prestataire externe avait accédé au système informatique de la banque pour copier les données du client avant de tenter d'extorquer de l'argent de la banque sous menace de transmettre les données à des tiers, dont des autorités fiscales. Les juges ont, à l'évidence, retenu qu'il avait accédé à ces données dans un but frauduleux[99]. La jurisprudence tend cependant à interpréter de manière large le concept d'accès « frauduleux » en considérant que tout auteur qui sait qu'il n'était pas censé accéder au système agit avec une

---

[91] R. GASSIN, op.cit.,n°195

[92] J-F. CASILE, op.cit,P.136,n°357

[93] M. PUECH remonte jusqu'au code d'Hammourabi.

[94] M. PUECH, « droit pénal général »,.éd. Litec 1988, n°509 et s

[95] E. GARÇON « code pénal annoté »,. 2ème éd. Par ROUSSELET, PATIN et ANCEL, art 1er n°77.

[96] G. CHAMPY, « La fraude informatique »,. Univ. D'Aix-Marseille, T. I , 1992. P. 244

[97] M. QUEMENER et Y. CHARPENEL, « Cybercriminalité », Economica, 2010, nº 312

[98] jurisprudence constante, voir p.ex. TA Lux., 16, 22 mai 2014, n' 1391/2014: TA Lux., 9, 3 juin 2015, n° 1669/2015, confirmé sauf quant à la peine par CSJ, 15 mars 2016, n° 161/16 V

[99] TA Lux, 18, 19 février 2015, nº 549/2015: « Or, en l'espèce, au vu de la matérialité des faits établis dans le chef du prévenu et des déclarations propres du prévenu, a lieu de retenir que le prévenu a accédé au système informatique de la banque dans un but frauduleux. ».

intention frauduleuse[100]. La pensée du législateur a été la suivante : agir frauduleusement est plus grave qu'agir intentionnellement et au mépris des droits d'autrui parce que, dans le premier cas, il faudrait violer un dispositif de sécurité alors que dans le second cas, on pourrait commettre le délit même si le système est ouvert au public[101].

B- Les usages frauduleux d'un STAD

L'usage consiste à « faire en sorte qu'une chose produise un effet souhaitable, soit en exerçant sur elle une action destructrice (consommer), soit en la faisant fonctionner, agir »[102], une notion introduite progressivement dans le champ répressif, substitue les éléments constitutifs de l'incrimination des infractions récemment apparues donne l'ordre à l'exercice d'une action.

L'accès ou le maintien frauduleux dans tout ou partie du système de traitement automatisé de données ne doit pas faire oublier l'existence d'un ensemble d'éléments. Dès lors que l'intrusion s'effectue dans une partie d'un système, il convient de rechercher dans quelle partie de l'ensemble elle s'est produite. Or, lorsque l'accès ou le maintien s'est réalisé sans influence sur les données, il semble difficile, dans des circonstances ordinaires, de constater l'infraction[103], ce qui ne sera pas le cas lorsque des données auront été introduites, effacées ou modifiées[104].

Cette approche présente l'avantage de saisir juridiquement la notion d'usage en informatique, laquelle ne deviendra pénalement répréhensible que si l'agent use d'un ou de plusieurs systèmes, dans le but d'en ressortir un enrichissement personnel, faut-il lié à l'appropriation ou à la destruction d'une donnée (a). Cette approche semble s'inscrire en complémentarité de certaines positions doctrinales pour qui « L'usage caractérise en la matière un acte, une action positive (utilisation) ou négative (modification), qui se réalise une fois que l'on est « entré » dans un « système de traitement automatisé de données »[105]. Un tel comportement n'a rien de frauduleux, il caractérise l'agissement de tout utilisateur normal. Il n'est frauduleux que par la qualité de celui qui en est à l'origine, qui outrepasse des droits qu'il ne possède peut-être même pas, ou par les modalités de l'acte elles-mêmes. L'on parlera alors de détournement ou de falsification[106], ou même de destruction des données (b).

a- Les atteintes aux système résultant de la manipulation de données de traitement

La fraude par manipulation informatique des systèmes de traitement de données admet une modification des données ou des informations afin d'obtenir un gain financier illicite[107]

L'article 607-5 C.P prévoit « Le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé de données est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement ».

---

[100] Dans cette approche, l'intention frauduleuse se confond avec le dol général, puisque le fait que l'accès se fasse « sans droit » implique qu'il soit frauduleux.

[101] M-P. LUCAS de LEYSSAC, in DIT n°88/2, commentaire de la loi n°88-19 du 5 janvier 1988.p. 20

[102] Dictionnaire, le petit Robert, Paris, 1996.

[103] On ne tient pas compte en l'espèce du cas où le système est sécurisé, de telle sorte qu'une intrusion dans le système serait immédiatement décelée. La victime disposant de connaissances en informatique constitue un cas d'espèce marginal.

[104] J-F. CASILE, op.cit, P. 81 et s.

[105] G. CHAMPY, « La fraude informatique »,. Th. Aix-en-Provence, 1992, presse universitaire d'Aix-Marseille, vol. II., p. 379.

[106] G. CHAMPY, op.cit., p. 379.

[107] U. SIEBER, « La délinquance informatique : les délits économiques liés à l'informatique et les atteintes à la vie privée »,. Précis et travaux. Fac. Dr. Namur. Trad. S. SCHAFF. Revue. M. BRIAT.1990. P. 7 et s

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

Cependant, Kao et Wang (2009) ont fait état de la grande difficulté de prouver la commission d'un cybercrime en n'utilisant que l'adresse IP et l'étampe temporelle (« *time stamp* ») qui sont supposés révéler la source d'un message. Les auteurs concluent que cette supposition est un mythe. Les cybercriminels savent brouiller les pistes en jouant précisément sur les adresses IP et l'étampe temporelle de manière à ce qu'ils ne puissent pas être retracés[108]. Une cyber-assurance donne une indemnisation en cas de dommages subis par un cyber-crime, mais la compagnie d'assurances n'a évidemment pas pour but de suivre les cybercriminels à la trace, de sorte que ceux-ci pourront éventuellement revenir visiter les ordinateurs. Mais regardons d'abord le phénomène lui-même de la cybercriminalité qui est multiforme et beaucoup plus complexe qu'il n'y paraît[109].

l'approche des Professeurs L. de BELLEFONDS et de M[e] HOLLANDE, qui intègre les programmes dans la catégorie des logiciels, harmonisant ainsi le sens technique et juridique de ces termesm[110], Selon ces auteurs, la définition du logiciel découlant de l'arrêté du 22 décembre 1981 relatif à l'enrichissement de la langue française ne fait pas autorité[111]. Pourtant, le logiciel défini juridiquement comme « l'ensemble des programmes, procédés et règles, et éventuellement de la documentation relatif au fonctionnement d'un ensemble de traitement de données », trouve son corollaire dans une définition technique semblable. En effet, le logiciel est traditionnellement défini comme « un ensemble de programmes destinés à effectuer un traitement sur un ordinateur », et le programme comme un algorithme destiné à une machine donnée, écrit dans un langage reconnu par cette machine »[112]. Le Professeur Gassin propose de considérer que la notion de fonctionnement d'un système « vise non seulement le fonctionnement d'un tel système (au sens de la définition du Professeur Devèze) dans sa totalité, mais encore celle de l'un quelconque de ses éléments, qu'il s'agisse des éléments matériels (ordinateurs, périphériques, organes de transmission...) ou des éléments immatériels (programmes, données informatives...)[113]

b Les atteintes aux systèmes résultant de l'altération de données traitées

L'article 607-3 du code pénal al 3 dispose que « La peine est portée au double lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système de traitement automatisé de données, soit une altération du fonctionnement de ce système ».

L'introduction, la détérioration, la suppression ou la modification des données, frauduleusement, dans un système de traitement automatisé expose son auteur à une peine d'emprisonnement d'un an à trois ans et/ou d'une amende de 10.000 à 200.000 dirhams[114]

Une remarque patente établie entre les dispositions des articles 607-6 et 607-3 c.p, il s'agit de l'absence du terme « *introduction frauduleuse de données* ». S'interpelle la question de préciser

[108] Da-Yu KAO et S-J. WANG (2009), «The IP address and time in cyber-crime investigation ». Policing, vol. 32, n°2, p. 194-208

[109] M. DION, « Éthique et criminalité financière »,. Harmattan, 2011, p. 187.

[110] X. LINANT de BELLEFONDS et A. HOLLANDE, « Pratique du droit de l'informatique », Delmas, 1998, n° 1016 et s

[111] X. LINANT de BELLEFONDS et A. HOLLANDE, *ibid*

[112] Selon le dictionnaire Larousse de l'informatique, l'algorithme est défini comme la description du schéma de réalisation d'un événement à l'aide d'un répertoire fini d'actions élémentaires nommées, à priori et à durée limitée dans le temps. L'écriture d'un algorithme se fait en utilisant des notations algorithmiques, c'est-à-dire d'un ensemble d'instructions élémentaires d'un langage de programmation

[113] R. GASSIN, op. cit., nº 166

[114] Art 607-6 C.P

alors et d'analyser si la suppression ou la modification de données est implicitement contenue dans le concept d'introduction, étant entendu que la suppression d'une donnée de programmation équivaut, dans une certaine mesure, à l'introduction d'une donnée. En effet, La condition primordiale, c'est qu'il convient d'assimiler la suppression ou la modification de données, à l'introduction implicite de données, en considérant que la modification d'une donnée de traitement, peut impliquer l'introduction d'une donnée traitée par une modification de sa mise en forme par exemple, sans nécessairement emporter de modification sur son sens[115].

La Cour énonça que « le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractérise le délit prévu à l'article 323-3 du Code pénal (l'article 607-6 du code pénal marocain) , sans qu'il soit nécessaire que ces modifications ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système, ni que leur auteur soit animé de la volonté de nuire»[116].

Notons que dans cette espèce, la Cour semble élargir la portée de l'article 323-3 du Code pénal (607-6 du code pénal marocain), tant au niveau de l'élément matériel de l'infraction qu'au niveau de l'élément moral[117].

Le législateur semble avoir dissocié le champ d'incrimination des articles 607-3 al 3 et 607-5 du code pénal , en les distinguant suivant l'objet de l'altération du système, laissant a priori à l'écart l'article 607-6 c.p qui concerne « le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient (...)». Pour certains auteurs, « *il n'y a pas lieu de distinguer entre les diverses catégories de données : il peut s'agir de données traitées comme le logiciel. Dans ce deuxième cas, la plupart du temps sauf intervention très finalisée et très sûre, c'est le traitement lui-même qui sera perturbé* »[118].

La convention de Budapest énonce que le fait d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques doit être une infraction pénale[119]. Par « suppression » des données informatiques, elle entend tout acte à la suite duquel ces données ne sont pas ou plus accessibles à la personne ayant accès à l'ordinateur ou au support sur lequel les données étaient stockées[120] Le droit allemand utilise la notion de « *Unterdrücken* », qui englobe de manière générale le fait de sortir l'objet de la sphère de possession inclut également le fait de cacher les données ou de les rendre autrement inaccessibles[121].

Les articles 509-1s. du Code pénal luxembourgeois, en revanche, utilisent la seule notion de « « suppression », en raison de ces différences terminologiques, un conflit peut naître entre le principe d'interprétation stricte du droit pénal et la nécessité d'une interprétation conforme au

[115] J.-F. CASILE, « le code pénal à l'épreuve de la délinquance informatique »,. Préf. G. FAURÉ, univ. D'Aix- Marseille. I.S.P.E.C. 2002. P.132.n°348.

[116] Cass crim., 8 déc, 1999, Gaz. Palais, 27-28 oct. 2000, jur., p. 45

[117] J-F. CASILE, « le code pénal à l'épreuve de la délinquance informatique »,. Préf. G. FAURÉ, univ. D'Aix- Marseille. I.S.P.E.C. 2002. P.134.n°352

[118] X. LINANT de BELLEFONDS et A. HOLLANDE, précité, n° 1408

[119] Art. 4 de la Convention de Budapest

[120] Rapport explicatif de la Convention sur la cybercriminalité, p. 12.

[121] D.KOCHHEIM, « Cybercrime und Strafrecht in der Informations- Kommunikationstechnik », 2. Auflage, C.H. Beck, 2018, n° 664

https://scopmajd.com/ « ISI: (0.360) « ISSN (Online): 3005-2033

droit international et européen. Cette dernière exigence invite cependant à l'interprétation le plus large possible de la notion de « suppression »[122]

Sources et references:

J-L. PUTZ, « Cybercriminalité : criminalité informatique en droit Luxembourgeois », éd. Larcier, Luxembourg, n°6. P.15.

P. Arrigo, « La cybercriminalité : vers une régulation internationale de l'Internet ? », Gaz. Pal. 16 oct. 2001, n°289. p. 35

Ph. BONFILS, L.GRÉGOIRE, « Droit pénal spécial », 25 janv. 2022, LGDJ. n°940.

V. MALABAT « Droit pénal spécial », 9ème éd. Dalloz, 2020. P.557.n°883.

H. ROBERT, « Réflexion sur la nature de l'infraction de blanchiment d'argent », JCPG 2008, 1 146, P. NÉRAC., «La répression de l'infraction générale de blanchiment », AJ pénal 2006, p. 440; M. SEGONDS, « Les métamorphoses de l'infraction de blanchiment... ou les enjeux probatoires de la lutte contre le blanchiment », AJ pénal 2016.

A-M. LARGUIER « Immunités et impunités découlant pour l'auteur d'une infraction d'une infraction antérieurement commise par celui-ci » JCP 1961, 1, 1601

les menaces c'est l'objet (ou la personne, ou l'évènement) qui peut causer un dommage (un impact négatif).

Eléments internes au sein de l'entreprise (son dispositif plus explicitement) qui pourraient être exploités par la menace identifiée

Art 12 al 1 Circulaire du président de l'Autorité de contrôle des assurances et de la prévoyance sociale n° AS/02/19 du 25 septembre 2019 relative aux obligations de vigilance et de veille interne incombant aux entreprises d'assurances et de réassurance et aux intermédiaires en matière d'assurances et de réassurance. B.O. n°6848 – 20 joumada I 1441.

V.MALABAT « Droit pénal spécial », éd. Dalloz. coll. « Hypercours »,6ème éd. 2013.n°831.

M. DAURY-FAUVEAU « Droit pénal spécial : livres 2 et 3 du code pénal : infractions contre les personnes et les biens 2010 »,. Préf. J -H. ROBER . éd.PUF.p.131.n°130

P. CAZALBOU « étude de la catégorie des infractions de conséquences : contribution à une théorie des infractions conditionnées »,. LGDJ. 2016, n°599.

D.KOCHHEIM, « Cybercrime und Strafrecht in der Informations- Kommunikationstechnik », 2. Auflage, C.H. Beck, 2018, n° 664

J-L. PUTZ, « cybercriminalité : criminalité informatique en droit Luxembourgeois »,.éd. Lefebvre Sarrut BELGIUM. 2019.p. 395-396, n°464

[122] J-L. PUTZ, « cybercriminalité : criminalité informatique en droit Luxembourgeois »,.éd. Lefebvre Sarrut BELGIUM. 2019.p. 395-396, n°464