LES CAPTATIONS ILLICITES DES SIGNAUX PARASITES ET LE NOUVEAU CODE PÉNAL

par

Michel VIVANT

Professeur à l'Université de Montpellier I
Doyen honoraire de la Faculté de Droit et des Sciences économiques

Les armées et les autres services de sécurité étant de très importants utilisateurs de systèmes d'information, ils doivent prendre en compte la protection technique et juridique de ces systèmes face aux agressions potentielles dont ils peuvent faire l'objet, notamment de la part de forces ou de services étrangers [1].

L'une de ces menaces qui pèsent sur les systèmes de traitement de l'information de la Défense est la captation illicite du rayonnement électromagnétique de ces systèmes, c'est-à-dire l'"écoute" à distance des signaux parasites qu'émet inévitablement tout dispositif électronique [2]. Bien qu'elle soit peu connue du grand public, cette forme d'espionnage électronique a toujours été considérée comme particulièrement dangereuse par les autorités gouvernementales car elle est très discrète (pas de branchement à effectuer, pas d'effraction) et donc quasiment impossible à détecter.

C'est aux Etats-Unis que cette menace a été étudiée avec le plus de soin, ce qui a conduit le Gouvernement fédéral à édicter un ensemble de normes spécifiant les caractéristiques de "discrétion" et de "non-compromission" électromagnétique [3] que doivent respecter les systèmes informatiques militaires pour être à l'abri de ces interceptions. La plus importante de ces normes est le NACSIM (National Communications Security Information Memorandum) 5100A, dit communément "norme TEMPEST" (Transient Electromagnetic Pulse Emanation Standard), dont le contenu est classifié. Cette norme américaine a été transposée au niveau de l'OTAN par la norme ASMG 720B. Et en France, une instruction interministérielle n°300 sur "les rayonnements compromettants" se réfère à des exigences techniques proches en ce qui concerne la protection électromagnétique des systèmes informatiques destinés à traiter des données classifiées.

Mais si la parade technique aux risques d'interception "Tempest" existe, elle ne peut pas être mise en oeuvre partout (en raison notamment de son coût) et elle ne dispense pas les organismes traitant des informations confidentielles (y compris les organismes privés) de se protéger juridiquement contre d'éventuelles interceptions électromagnétiques. C'est cet aspect juridique d'un problème considérable pour la Défense que le Doyen Michel Vivant aborde dans l'article ci-dessous, à la lumière du nouveau Code pénal qui est en vigueur depuis le 1er mars dernier.

Bertrand WARUSFEL

---

1 On a, par exemple, déjà noté, dans cette revue, la rédaction de l'article 411-9 du nouveau Code pénal dont le second alinéa punit de manière aggravée les actes de sabotage s'exerçant, notamment, sur des systèmes de traitement de l'information lorsquils ont été commis *"dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger".*

2 Cf. par exemple, W. Van Eyck, "Rayonnement électromagnétique d'information par des terminaux cathodiques", *Actes du congrès SECURICOM* 1985, p. 299

3 Il s'agit de deux caractéristiques complémentaires : la "discrétion" consiste à limiter au maximum l'importance des radiations émises par l'ordinateur, la "non-compromission" correspond au fait que les radiations, malgré tout émises, ne puissent pas permettre de reconstituer le contenu des informations traitées dans l'ordinateur.

La tempête n'est pas dans un verre d'eau, mais elle ne se fait guère sentir, pour l'heure, au-delà d'un cercle véritablement restreint de spécialistes informés. Et pourtant, l'"effet Tempest" est une réalité dont l'exploitation criminelle est à redouter. En effet, tout matériel ou système qui traite ou transmet, sous forme électrique, des informations est le siège de perturbations électromagnétiques et émet, de la sorte, des signaux parasites qui se propagent par rayonnement et par conduction [1]. Or certains de ces parasites sont représentatifs des informations traitées et peuvent être captés et analysés afin de restituer l'information qu'ils véhiculent [2].

Par cette captation, il n'est plus de lieux publics ou privés qui soient à l'abri du plus efficace espionnage.

Les micros placés sur les ordinateurs qui avaient été utilisés contre le matériel américain lors de la guerre du Viêt-nam prennent brutalement un visage archaïque [3]. On chuchote même, semble-t-il non sans raisons, qu'un des lieux les plus sensibles de la planète est aujourd'hui une des cibles privilégiées de cette captation pirate et le pire est que la grande criminalité de droit commun paraît bien s'intéresser à ces développements nouveaux de la technologie.

Bien sûr, suivant le jeu traditionnel du blindage et du projectile, la première réponse à trouver est technique (utilisation de matériels protégés contre la menace de captation, installation des matériels dans des zones protégées, chiffrement de l'information mise en mémoire ou traitée par l'ordinateur,...) et le fait est que, dans tous les grands pays développés, des services spécialisés travaillent à l'étude du phénomène, aux moyens de le combattre, et préconisent des matériels aptes, en l'état actuel des choses, à repousser les agressions. Les Communautés européennes poussent à une politique de sécurité [4].

Mais la question se pose aussi de savoir si, sur le terrain du droit, une réplique pénale peut être trouvée dans l'arsenal positif.

1. La réponse affirmative ne fait pas de doute quand la captation n'apparaît que comme un nouveau mode d'accès à l'information tel que traditionnellement criminalisé ; ainsi en est-il quand on peut y voir un acte d'espionnage au sens le plus classique du terme [5]. L'observation vaut encore si la captation réalise la violation d'une "valeur" que le droit entend sanctionner ; ainsi en est-il quand le Code réprime, sans qu'il soit question d'espionnage, les atteintes portées à un secret comme celui de la défense nationale [6] ou, dans un autre registre, et pour autant qu'il y ait correspondances, les atteintes au secret des correspondances [7] (mais non comme on pourrait s'y attendre, les atteintes à la vie privée trop restrictivement définies

1 C'est là l'"effet Tempest".

2 C'est la captation... qui fait problème. Le rapport sur "La criminalité informatique", publié en annexe de la recommandation n° R (89) 9 du Comité des ministres du Conseil de l'Europe sur *"la criminalité en relation avec l'ordinateur"*, y fait une discrète allusion ; il vise, en effet, comme *"interception non autorisée", "l'interception des radiations et des champs électroniques entourant l'ordinateur"* (II, 2, f).
On ajoutera que, si aujourd'hui le phénomène n'est, comme il vient d'être dit, réellement connu que des spécialistes, certains écrits destinés au grand public en ont, pourtant, déjà fait état ; ainsi, par exemple, J. Denis-Lempereur, Les oreilles de l'État, *Science et Vie*, juin 1992, pp. 104 et ss.

3 Voir J.-M. Chabanas, La criminalité en ligne, *Le Monde*, Dossiers et documents, sept. 1982, p. 110 et ss.

4 Cf. Décision du Conseil du 31 mars 1992 en matière de sécurité des systèmes d'information (*JOCE* n° L 123 du 8 mai 1992, p. 19).

5 Articles 411-1 et ss. du nouveau Code pénal (nCP).

6 Articles 413-9 et ss. nCP qui entendent sanctionner la négligence du dépositaire d'une information secrète, notamment prenant la forme de "données informatisées", intéressant la défense nationale (comp. art. 75 et 76 2° CP).

7 Article 226-15 nCP al..2 qui punit "le *fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions*" (les articles L. 41 du Code des postes et télécommunications et 186 du Code pénal étaient de portée bien plus restreinte puisque supposant un auteur agent de l'exploitation du réseau ou d'un service de télécommunication).

pour notre propos [8]). Mais à la vérité, cela n'est que périphérie [9].

2. La question de savoir si le droit pénal répond bien au phénomène de la captation illicite mérite d'être plus franchement posée, à savoir : le fait même de capter les signaux parasites peut-il être incriminé ?

On observera, puisqu'un nouveau Code pénal vient d'être adopté, que, curieusement, les travaux préparatoires qui ont conduit à celui-ci n'en ont rien dit, alors même que le phénomène, fut-il peu connu, prenait de l'ampleur. Ce silence a-t-il un sens ? Signifie-t-il que le législateur a ignoré le phénomène ? Ou, s'il ne l'a pas ignoré, faut-il penser qu'il a considéré que la captation ne devait pas être sanctionnée ou tout au contraire que sa criminalisation était acquise ? Il serait certainement hasardeux de se lancer dans une recherche de cet ordre, nécessairement divinatoire.

Il est plus assuré d'examiner les textes tels qu'ils sont issus d'abord de la loi du 5 janvier 1988 relative à la fraude informatique [10], ensuite aujourd'hui du nouveau Code pénal qui a repris les premiers moyennant quelques modifications [11]. Et, puisque, contrairement à ce que projetait la "proposition Godfrain" originaire, la captation n'est pas expressément visée [12] et comme notre propos n'est pas de "forcer" le texte pénal, même au prétexte de moralisation et sous couvert de modernité [13], notre démarche consistera, très simplement, à nous demander si l'article 323-1 de ce nouveau Code pénal, repris pour l'essentiel de l'article 462.2° CP, qui incrime l'accès - et le maintien - frauduleux dans un système, peut trouver à s'appliquer au cas de la captation de signaux parasites : capter est-ce donc accéder à un système au sens de la loi ?

Nous nous efforcerons de répondre à cette question selon une démarche classique, c'est-à-dire respectueuse [14] des principes d'interprétation stricte , soucieuse de cohérence et consistant sans fioritures à examiner tour à tour élément matériel (I) et élément moral (II). On rappellera pour la commodité du lecteur que l'article 323-1 nCP dispose : *"Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100.000 F d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200.000 F d'amende"* [15].

I. LA CAPTATION DES SIGNAUX PARASITES ET L'ÉLÉMENT MATÉRIEL DE L'ARTICLE 323-1 DU NOUVEAU CODE PÉNAL

1.1. Les deux textes, celui du nouveau Code pénal, comme le précédent, visant l'accès à tout ou partie d'un système, une

8 Articles 226-1 et ss. nCP qui visent, en effet, captation, enregistrement,... de "paroles" ou d'"images". Ce qui n'interdit pas, d'un point de vue philosophique et/ou *de lege lata*, d'analyser de telles agressions comme constitutives en soi d'agressions contre la vie privée, ou, peut-être, plus justement contre la *privacy* (en ce sens Rapport du Comité européen pour les problèmes criminels, précité note 2).

9 Toute une série de dispositions relatives à la protection des informations peuvent, d'ailleurs, être encore mobilisées : ainsi, très spécifiquement, de l'article 226-17 nCP qui incrimine "*le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment qu'elles ne soient déformées, endommagées, ou communiqués à des tiers non autorisés est puni...*" (Comp. art. 42 de la loi dite "Informatique et libertés" du 6 janvier 1978) ; ainsi, plus largement et en aval de la captation, des textes frappant toute révélation indue, de la livraison de secrets de la défense (encore...) à une puissance étrangère à la "*révélation d'une information à caractère secret*" par celui qui la détient (telle qu'instaurée par l'article 226-13 nCP).
D'intéressants développement dans le remarquable ouvrage du professeur Sieber, *The International Handbook on Computer Crime*, Chichester, John Wiley & sons, 1986, spéc. développements sur le "*computer espionnage*" (p. 52 et ss.) et notamment : "*Protection of Special Secrets and Relationships*" (p. 60 et ss.).

10 Dite "Loi Godfrain".

11 Art. 323-1 et ss. : "*Des atteintes aux systèmes de traitement des données*".

12 La proposition envisageait l'adoption d'un texte frappant des peines du vol simple "*quiconque aura capté délibérément sans droit des données ou programmes enrenregistrés*".

13 Entre les "arabesques" et la défense des libertés, c'est cette dernière qui doit être clairement privilégiée.

14 Qui n'exclut pas - faut-il le rappeler ? - une lecture téléologique des dispositions légales.

15 L'article 462-2° CP (issu de la loi du 5 janvier 1988) se présentant, quant à lui, ainsi : "*Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2.000 à 50.000 F ou de l'une de ces peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenue dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10.000 à 100.000 F*".

décomposition bipartie s'impose tout naturellement. Peut-on parler d'accès à propos de la captation de signaux parasites ? Si accès il y a, est-ce bien de l'accès à un système dont il s'agit ?

1.2. Accès : la captation peut-elle être qualifiée d'accès ?

Ou encore : qu'est-ce qu'un accès ? Une pénétration physique ? La réponse à la première question posée est alors indiscutablement négative. Accès intellectuel ? Pénétration ? La vision de l'incrimination change du tout au tout...

L'analyse la plus fine - et partant la réponse la plus ferme - peuvent certainement être trouvées sous la plume du professeur Gassin [16] qui, disséquant le texte [17], fait observer que c'est essentiellement l'accès à l'immatériel qui est visé, autrement dit l'accès à la capacité de réaliser des opérations intellectuelles dont est doté le système.

Cette analyse est, en tout cas, en résonance directe avec ce qui ressort des travaux parlementaires ayant conduit à la loi de 1988. En effet, à l'époque, la question de la captation de signaux parasites avait été, contrairement à 1992, directement abordée - même si elle ne fut pas toujours précisément qualifiée - et cela dans un sens favorable à la répression. Dans son rapport à l'Assemblée [18], M. André écrit ainsi : "*Est visé tout mode d'accès frauduleux, y compris par captation des signaux émis (notamment par rayonnement)*". De même, dans son rapport devant le Sénat [19] le sénateur Thyraud fait également référence aux "*rayonnements émis par les système de télétraitement*". Sans doute, la référence à un accès "direct ou indirect" portée par le texte voté en première lecture par l'Assemblée nationale, a, par la suite, disparu lors du premier passage devant le Sénat et l'on pourrait être tenté d'y voir une réduction de la portée du texte alors voté. Mais tout au contraire, le rapporteur au Sénat [20] devait expliquer très clairement que l'intention de la Haute Assemblée n'était pas de restreindre mais d'élargir l'infraction[21]. Aussi ne faut-il pas s'étonner de constater que la doctrine quasi unanime se soit prononcée dans le même sens que le professeur Gassin [22].

1.3. Accès "*dans tout ou partie d'un système de traitement autorisé de données*" : la plupart des commentateurs de la loi insistent sur la nécessité qu'il y ait eu accès à un "*système de traitement automatisé de données*" en tant que condition préalable du délit [23].

Autrement dit, l'infraction ne pourrait résulter d'un accès à un élément informationnel isolé, séparé d'un système.

Le législateur ayant renoncé à définir le système, quelques incertitudes pourraient certes se manifester mais une conception large du "système" paraît s'imposer. L'ensemble de la doctrine reprend en effet la définition que souhaitait lors du vote de la loi de 1988 le Sénat (ensemble composé d'une ou plusieurs unités de traitement, mémoire, logiciel, données, etc) en y ajoutant les transmissions et les périphériques d'entrée ou de sortie.

Les signaux parasites étant émis par la carte graphique, il ne fait a priori aucun doute que leur captation réalise bien l'"*accès à tout ou partie d'un système de traitement automatisé de données*".

Si les rayonnements captés sont émis par le seul système de transmission un doute peut, il est vrai, surgir. On peut soutenir que les transmissions prises isolément ne constituent pas un système ou encore qu'elles

16 R. Gassin, Fraude informatique, Encycl. Dalloz Droit pénal, n° 99 et s.

17 L'article 462-2° CP en l'occurrence, mais sans que ceci ait d'incidence sur le raisonnement mené.

18 N° 744, seconde session ordinaire de 1986-1987, P. 13.

19 N° 3, première session ordinaire de 1987-1988, p. 53.

20 Rapport précité, p. 68.

21 Ce qui a, d'ailleurs, été fait par l'adjonction du "maintien" à l'"accès" seul visé par le texte de l'Assemblée.

22 Voir notamment : G. Champy, La fraude informatique, P.U. d'Aix- Marseille, 1992, p. 161 et ss. ; J. Devèze, Infractions en matière informatique, *Juris-Classeur pénal*, n° 42 ; M.-P. Lucas de Leyssac. Fraude informatique... Loi du 5 janvier 1988, *Rev. droit de l'informatique et des télécoms.* 1988, n° 2, qui considère qu'est visé "*l'accès à un système par captation de signaux émis*" ; M. Vivant, C. Le Stanc et autres, *Lamy Informatique*, éd. de 1993, n° 2067, qui visent expressément parmi les agissements que peut couvrir le texte le fait de "*capter des rayonnements*". *Contra* J.-P. Bufelan-Lanore, La protection des biens informatiques, *Les Petites Affiches* 1990, n° 81, P. 27, sur la considération que le texte voté en 1988 ne reprenait pas les dispositions de la proposition de loi relatives à l'accès.

23 Ainsi R. Gassin, *op. cit.* ; H. Crize, L'apport du droit pénal à la théorie générale du droit de l'informatique, *J.C.P.* 1988, I. 3333 ; M.-P. Lucas de Leyssac, *op. cit.* ; G. Champy, *op. cit.*

constituent un système de transmission "*distinct du*" système de traitement seul visé au texte. A la première objection, on doit toutefois répondre d'abord que les transmissions sont nécessairement "*reliées*" à un système, ensuite que l'accès peut ne concerner qu'une partie de système. Quant à la seconde objection, présentée par madame Lucas de Leyssac et point retenue par les autres commentateurs, elle s'appuie sur une interprétation, nous semble-t-il, exagérément exégétique et cela plus encore aujourd'hui qu'avec la symbiose des techniques, les frontières entre traitement "*statique*" et communication perdent toute réalité.

1.4. L'élément matériel de l'article 323-1 nCP recouvre ainsi, nous semble-t-il, sans matière à polémique, la captation de signaux [24].

II. LA CAPTATION DES SIGNAUX PARASITES ET L'ÉLÉMENT MORAL DE L'ARTICLE 323-1 DU NOUVEAU CODE PÉNAL

2.1. Reste que l'infraction d'accès (et de maintien) indus n'est pas une infraction matérielle. Tout accès n'est pas frappé.

2.1.1. L'accès doit, d'abord être volontaire. Mais cette condition ne nous paraît pas susceptible de faire problème dès lors que la captation suppose l'installation et l'utilisation d'un matériel particulier... et qu'on les imagine mal faites pas inadvertance !

Si, par extraordinaire, il pouvait en aller autrement, il resterait qu'à partir du moment où l'auteur de la captation inopinée (!) prendrait conscience de son acte, il y aurait "*maintien*" volontaire et donc matière à application de la loi, puisque le texte vise "*le fait d'accéder ou de se maintenir*".

2.1.2. Mais, à raisonner sur l'accès, l'accès incriminé est l'accès frauduleux ("*Le fait d'accéder ou de se maintenir, frauduleusement ...*"). Il doit donc encore - autre manière de formuler l'exigence légale - être réalisé en conscience de son irrégularité, c'est-à-dire en sachant qu'il est contraire à la volonté du "*maître*" du système. Là encore, pourtant, cette condition ne devrait pas poser de problèmes. Une captation ne se fait pas inopinément, elle ne se fait pas non plus dans une virginale innocence... Celui qui exploite l'effet Tempest sait très bien ce qu'il fait et mène consciemment une agression contre un système qu'il sait ne pas lui être ouvert.

Sans doute, si l'accord se fait généralement chez les auteurs pour dire que le texte légal joue sans qu'il soit besoin de supposer le système protégé [25], l'absence de dispositif de sécurité peut, en première approche, être perçue comme faisant obstacle à ce que l'accès puisse être qualifié de frauduleux. Mais l'observation ne nous paraît guère résister à l'examen. Le fait qu'un système soit librement accessible n'implique évidemment en rien l'autorisation d'en capter les signaux parasites compromettants. Le fait que le maître du système n'ait pas pris des mesures de protection technique contre la fraude n'implique pas davantage l'autorisation de pirater...

2.2. L'élément moral constitutif de l'infraction de l'article 323-1 nCP nous paraît ainsi facilement présent dans l'acte de captation de signaux parasites.

2.3. Élément matériel et élément moral :

Cette captation de signaux parasites exploitant l'effet Tempest est donc, selon nous, en l'état de notre droit et en l'absence de dispositions expresses (de fait inutiles), parfaitement incriminable.

---

24 Sauf à noter une difficulté si captation et décryptage sont dissociés et accomplis par deux personnes différentes. Les deux actes accomplis de concert, il ne devrait y avoir aucun mal à tenir les deux acteurs pour co-auteurs du délit d'accès frauduleux (à supposer l'élément moral caractérisé ; voir ci-après). Dans le cas contraire, c'est-à-dire si l'auteur de la captation communique son enregistrement à un tiers indépendant pour le décrypter, les choses sont moins claires quant au sort de ce tiers... il faudra sans doute raisonner en termes de recel : voir *infra* n°10.

25 En ce sens, notamment : J. Devèze, *op. cit.* ; R. Gassin, op. cit. ; M. Vivant, C. Le Stanc *et alii*, *op. cit. Contra*, cependant, semble-t-il, G. Champy, *op. cit.*, pp. 80 et ss. On notera, d'ailleurs, à cette occasion que, si le rapport du Comité européen pour les problèmes criminels (précité notes 2 et 9) préconise l'adoption d'une disposition spécifique visant "*l'interception, sans droit et par des moyens techniques, de communications à destination, en provenance et au sein d'un système ou d'un réseau informatique*" (II, 2, f), n'est certainement pas sans rapport avec le fait qu'il suggère d'adopter un texte incriminant l'accès aux systèmes "*par violation des régles de sécurité*" (II,2,e).

Si, un jour, les tribunaux répressifs devaient être saisis d'un tel dossier, ils trouveraient dans l'arsenal juridique existant [26] le moyen de sanctionner de tels agissements.

La seule lacune que pourrait révéler la loi concernerait le cas de celui qui aurait reçu communication des signaux captés à l'effet de les décrypter pour son propre compte, sans avoir lui-même procédé à la captation [27]. Difficile en ce cas de le tenir pour coupable d'un accès illicite. Impossible selon nous - qui refusons ce jeu dangereux [28] - de "découvrir" un vol d'information, pour conclure au recel d'information. La solution est cependant vraisemblablement là, à savoir dans la qualification de recel. Sans doute, dans une conception traditionnelle supposant un chose "provenant" d'un délit [29] les choses ici recelées étant les données, il est difficile de soutenir que ces choses soient l'objet même du délit initial, tout défini comme un accès indu. Mais les termes de la loi sont tels aujourd'hui que l'incrimination de recel peut certainement être retenue dans le cas particulier qui retient notre attention, puisque l'article 323-1, al. 2, du nouveau Code pénal vise "*le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit*".

2.4. Il est de bon ton de dire que le droit est en retard sur les phénomènes sociaux et/ou techniques. Si ces quelques lignes consacrées à une technique en développement et à une pratique criminelle... à naître, pouvaient avoir démontré que le droit est à même d'anticiper développements techniques et comportements sociaux de manière telle que précisément ne puissent "bénéficier ... d'un délit" ceux qui auraient imaginé d'user du progrès pour cultiver leur déviance, elles n'auraient point été inutiles : pour clarifier certaines choses (espérons-le) mais aussi pour démontrer que le droit peut, aux antipodes des idées reçues, être en avance...

M.V.

---

26 Arsenal juridique qu'offre, au moins, le droit pénal français.

27 Voir *supra* n°7 note 25.

28 La qualification nous paraît fantaisiste (voir là - dessus M. Vivant, C. Le Stanc et alii, *Lamy Informatique* , précité, 1993, n° 2036, et ss. et 2058) mais, plus gravement, conduisant par un jeu de l'esprit à incriminer ce qui ne devrait pas l'être, elle met en péril gravement les libertés.

29 Conception reçue dans l'article 323-1 al. 1er nCP.