PROCÉDURE PÉNALE ET TECHNOLOGIES DE L'INFORMATION : De la Convention sur la Cybercriminalité à la Loi sur la sécurité quotidienne

par
Bertrand WARUSFEL,
Maître de conférences à la faculté de droit de l'Université Paris V,
Directeur-adjoint de la revue Droit & Défense

L'intense agitation créée à la fin 2001 par les attentats perpétrés aux États-Unis le 11 septembre a masquée le fait que certaines des dispositions les plus spectaculaires qui furent ajoutées en urgence au projet de loi sur la sécurité quotidienne (LSQ) [1] s'inscrivaient, en réalité, dans un contexte juridique et politique plus large : celui de l'adaptation du droit et de la procédure pénale aux nouvelles technologies de l'information. En effet, à quelques jours de l'adoption définitive de la LSQ française, les États membres du Conseil de l'Europe signaient définitivement une Convention longuement préparée et âprement discutée : la Convention sur la cybercriminalité [2]. Et cette convention faisait, elle-même, suite à une recommandation du Conseil de l'Europe, passée assez inaperçue en 1995 et pourtant consacrée au sujet essentiel des problèmes de procédure pénale liés à la technologie de l'information [3].

I. La nécessité d'adapter la procédure pénale aux technologies de l'information

La recommandation R(95)13 du Comité des Ministres du Conseil de l'Europe du 11 septembre 1995 est sans doute le premier document international à avoir fait l'inventaire des incidences que l'utilisation croissante des nouvelles technologies de l'information et de la communication (NTIC pour reprendre l'acronyme couramment utilisée aujourd'hui) ne manquerait pas de poser aux règles classiques de la procédure pénale.

Les principales recommandations formulées par ce texte à destination des États membres portaient sur les points suivants :

- rendre possible, dans le cadre d'enquêtes pénales, des perquisitions et des saisies informatiques, de façon à *"permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie."* (art. I.2.) ;

[1] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *J.O.R.F.*, n°266, 16 Novembre 2001, pp. 18215 et s.. Pour un résumé de l'ensemble de ces amendements introduits après le 11 septembre, cf. notre chronique, Bertrand Warusfel, "La loi sur la sécurité quotidienne renforce les mesures anti-terroristes et de lutte contre certaines formes majeures de délinquance", *Droit & Défense*, n° 2001/4, pp. 45-47.

[2] La Convention sur la cybercriminalité a été adoptée par le Comité des Ministres du Conseil de l'Europe à l'occasion de sa 109e Session, le 8 novembre 2001 et ouverte à la signature à Budapest, le 23 novembre 2001, à l'occasion de la Conférence Internationale sur la Cybercriminalité.

[3] Conseil de l'Europe, Recommandation n° R(95)13 du Comité des Ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée par le Comité des Ministres le 11 septembre 1995.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

- adapter les règles relatives aux interceptions [4] pour permettre l'interception des communications informatisées, la collecte et la conservation des *"données de trafic"* [5] (art. II) ;

- pouvoir obliger certaines personnes (notamment les prestataires de services et les opérateurs, mais aussi les personnes faisant elles-mêmes l'objet d'une enquête) à remettre des éléments informatiques susceptibles de servir de preuve (art. III) ;

- adapter les règles de procédure aux moyens de preuve électronique (art IV) ;

- faire en sorte de *"minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales"* (art. V) ;

- organiser la coopération internationale et l'entraide judiciaire de manière à permettre, en cas d'urgence, des perquisitions dans des systèmes informatiques situés sous une juridiction étrangère (art. VII).

La Convention sur la cybercriminalité signée en novembre 2001 après des travaux commencés en 1996, a pour une large part repris à son compte les orientations de cette recommandation de 1995, auxquelles elle donne désormais force contraignante à l'égard des États membres.

En effet, il faut distinguer au sein du dispositif de la nouvelle Convention deux catégories de dispositions : d'une part, des dispositions de droit pénal matériel obligeant les États à poursuivre certaines infractions spécifiques aux réseaux numériques, d'autre part, des dispositions procédurales

Or, ce n'est pas au titre de la première catégorie que notre droit français devrait connaître d'importantes évolutions. En effet, on peut estimer que, dans l'ensemble, le droit pénal français est déjà largement conformes aux exigences de la Convention en ce qui concerne les incriminations propres à la cybercriminalité. S'agissant des infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques (titre I), les articles. 343-1 à 343-7 du code pénal issus de la "loi Godfrain", ainsi que le second alinéa de l'article 226-15 devraient couvrir le champ défini par la Convention ; il en va de même en ce qui concerne la falsification informatique (art. 7) qui paraît pris en compte par la définition large du faux donnée par l'article 441-1 [6]. De même, les dispositions pénales françaises

[4] Régies en France par la loi loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, laquelle distingue les *"interceptions judiciaires"* (utilisables en procédure pénale) des *"interceptions de sécurité"* (décidées par le Premier ministre au profit des services de renseignement et de sécurité).

[5] On appelle "données de trafic" les données techniques recueillies automatiquement par les prestataires de communication (tels que les opérateurs de télécommunications) à l'occasion de toute communication passée sur un réseau. Ces données de trafic ne donnent pas le contenu de la communication, mais permettent généralement d'en connaître certaines caractéristiques (identification de l'émetteur et du récepteur, durée, …).

[6] Sur l'ensemble des infractions pénales en relation avec les nouvelles technologies, cf. notre article, "Les technologies de l'information dans le nouveau Code pénal", *Droit de l'Informatique et des Télécoms*, 1994/2.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

réprimant la pornographie infantile (Titre III) et les atteintes aux droits de propriété intellectuelle (Titre IV) paraissent susceptibles de couvrir également les actes commis par le biais de l'Internet. Restent seulement des interrogations sur la nécessité de renforcer les textes existants en ce qui concerne ce que la Convention appelle précisément la *"fraude informatique"* (art. 8) et les différents actes réunis sous le terme d'*"abus de dispositifs"* (art. 6).

En revanche, les dispositions de la Convention relatives à la procédure et qui sont directement inspirées des principes fixés en 1995, appellent dans de nombreux cas une transposition législative en droit français.

La Convention impose, en particulier, aux États parties de se mettre en mesure de disposer pour enquêter sur les infractions informatiques ainsi que sur la commission par informatique d'infractions classiques [7], des moyens suivants :

- pouvoir d'enjoindre *"la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification"* et la sauvegarde de ces données conservées pendant une durée maximale de 90 jours, éventuellement renouvelable (art. 16.1) ;

- obligation imposée aux fournisseurs de services de conserver et de communiquer les données de trafic pour permettre, notamment, *"l'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise"* (art. 17) ;

- pouvoir d'enjoindre à tout utilisateur de communiquer des données informatiques en sa possession et à tout fournisseur de service de communiquer les données relatives à ses abonnés (art. 18) ;

- droit de perquisitionner et d'accéder à tout système informatique installé sur le territoire national, et de saisir ou de copier toute information numérique qui y est stockée (art. 19) ;

- pouvoir de collecter (ou de faire collecter par les fournisseurs de service) en temps réel les données de trafic (art. 20) ;

- et *"relativement à un éventail d'infractions graves à définir en droit interne"*, le pouvoir d'intercepter (ou de faire intercepter) le contenu de certaines communications (art. 21).

Sauf en ce qui concerne le dernier aspect, que l'on peut considérer comme déjà mis en œuvre par les dispositions du code de procédure pénale issu de la loi du 10 juillet 1991 sur le secret

[7] L'article 14 de la Convention définit ainsi le champ d'application des nouvelles dispositions procédurales qu'elle prévoit : *"chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 : (a) aux infractions pénales établies conformément aux articles 2-11 de la présente Convention ; (b) à toutes autres infractions pénales commises au moyen d'un système informatique ; et (c) à la collecte des preuves électroniques de toute infraction pénale."*

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

des télécommunications, la plupart des autres dispositions devrait donc nécessiter une transposition spécifique. Et la première vague de ce mouvement de transposition a commencé (avant même que la Convention ne soit encore entrée en vigueur) avec les dispositions supplémentaires ajoutées au projet de la loi sur la sécurité quotidienne qui concernent d'une part la collecte et la conservation de données de trafic à des fins probatoires et d'autre part l'accès aux données chiffrées.

II. La collecte et la conservation de données de trafic à des fins probatoires

L'article 29 de la loi du 15 novembre 2001 a introduit notamment deux nouveaux articles L. 32-3-1 et L. 39-3 au Code des postes et télécommunications. Ces articles, tout en reconnaissant que, par principe, tout opérateur se doit *"d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée"* (art. L. 32-3-1.-I.), vont permettre en réalité - par un jeu de dérogations mises en œuvre par un prochain décret en Conseil d'État - d'imposer désormais aux opérateurs de télécommunication la conservation durant une période maximale d'un an de certaines de ces données *"relative à une communication"* .

2.1. Une obligation de conservation des données de trafic

Cette obligation s'imposera, non seulement aux opérateurs de réseaux de télécommunication au sens du code des postes et télécommunications mais également à l'ensemble des fournisseurs d'accès à l'Internet (souvent dénommés FAI) qui sont visés explicitement par ces dispositions dans la mesure où ils appartiennent à la catégorie des *"personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée"* visée au nouvel article 43-7 de la loi du 30 septembre 1986 relative à la liberté de communication (tel qu'elle a été complétée par la loi du 1er août 2000).

Cette conservation de données - qui devraient être ce que la Convention sur la cybercriminalité dénomme *"données de trafic"* [8]- aura pour but *"de permettre, en tant que de besoin,* [leur] *mise à disposition de l'autorité judiciaire… pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales"* (art. L. 32-3-1.-II.). Et tout manquement des opérateurs et des fournisseurs d'accès à cette obligation de conservation est passible d'un an d'emprisonnement et de 75 000 € d'amende, ainsi que d'une peine d'interdiction professionnelle de cinq ans à l'encontre des personnes physiques responsables (art. L. 39-3).

Par ces dispositions, le législateur français a donc pour objectif de se plier par avance à l'obligation qu'imposera, dès son entrée en vigueur, la Convention du Conseil de l'Europe, en ce qui concerne en particulier la possibilité d'exiger des opérateurs la communication des données de trafic dans le cadre d'une enquête pénale. Cela va, de même, dans le sens du 12ème

[8] Le IV de l'article L. 32-3-1. précise, d'ailleurs, explicitement, que ces données conservées *"portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers"* et qu'elles *"ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications."*

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

point de la Recommandation de 1995 qui précisait que *"des obligations spécifiques devraient être établies pour les fournisseurs de services qui offrent des services de télécommunication au public via des réseaux de communication publics ou privés, de délivrer l'information nécessaire, lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur."*

2.2. Des données accessibles non seulement à la justice, mais également à certains services de contrôle

Pourtant, à peine adoptées, ces dispositions ont fait l'objet d'un complément législatif, tout aussi hâtif, à l'occasion de l'adoption de la loi de finances rectificative pour 2001 [9]. L'article 62 de cette loi vient en effet conférer explicitement aux services des douanes (via une modification de l'article 65 du code des douanes) ainsi qu'aux services fiscaux (via la modification de l'article L. 83 du livre des procédures fiscales) et à la Commission des opérations de bourse (via une modification de l'article L. 621-10 du code monétaire et financier) le pouvoir déjà reconnu à l'autorité judiciaire de se faire communiquer les dites données de trafic que les opérateurs et fournisseurs de service vont désormais avoir l'obligation de conserver. Mais, ce faisant, ce "cavalier budgétaire" a discrètement élargi le champ d'application des obligations de conservation des données de trafic.

En effet, les modifications introduites dans les trois codes par cet article 62 de la loi de finances rectificatives mentionnent outre les opérateurs de télécommunications et les fournisseurs de services visés par l'article 43-7 de la loi de 1986, les prestataires visés par l'article 43-8 de cette dernière loi, c'est-à-dire les "hébergeurs" de sites Internet [10].

D'autre part ces organismes de contrôle administratif se voient reconnaître la possibilité de faire jouer leur droit de communication à l'égard de ces données de trafic, alors que ce droit de communication n'a pas pour objet la seule poursuite d'infractions pénales. Il s'agit donc d'un second élargissement notable de la portée de l'obligation de conservation créée par la LSQ, même si le Conseil Constitutionnel saisi de cet article de la loi de finances rectificatives l'a validé par sa décision du 27 décembre 2001 [11], ne l'a pas relevé et s'est contenté d'affirmer – dans un considérant elliptique – que le droit d'accès à ces données *"ne peut s'exercer que « dans le cadre de l'article L. 32-3-1 du code des postes et télécommunications »"*, sans que l'on puisse savoir s'il faudrait y voir une forme de réserve d'interprétation [12].

Toujours est-il que ce repentir législatif laisse quelque peu rêveur, d'autant que - comme le fait remarquer un récent commentaire de cette disposition [13]- on pourrait même se demander si par combinaison entre les dispositions usuelles régissant les délais de conservation des

[9] Loi de finances rectificative pour 2001, *JORF*, n° 1276 du 28 décembre 2001, p. 21133.

[10] L'article 43-8 créé par la loi n°2000-719 du 1er août 2000 vise *"les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services"*.

[11] Décision n° 2001-457 DC du 27 décembre 2001, *JORF*, 29 décembre 2001, p. 21172.

[12] Selon laquelle les administrations concernées ne pourraient user de leur droit de se faire communiquer les données considérées que dans les seuls cas et pour les seuls objectifs – à savoir des enquêtes pénales - prévus par l'article créé par la LSQ.

[13] Cf. Joël Heslaut, "La conservation des données de connexion étendue à tout l'Internet ?", *Les Échos*, 15-16 février 2002, p. 54.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

pièces communicables aux administrations fiscales et douanières, les opérateurs et les hébergeurs ne vont pas être contraints par prudence à conserver, non plus durant un an, mais durant trois ans, les données de trafic ? Si tel était le cas, cela viderait totalement de son sens, l'obligation de principe qui demeure dans l'article L.32-3-1 de faire disparaître ou de rendre anonyme, sauf cas particulier, toutes les données recueillies à l'occasion des communications.

III. La délicate question de l'accès aux données chiffrées

Moins médiatique peut-être que ce sujet de la conservation et de l'accès aux données de trafic et de connexion, la question de l'accès et de la "mise au clair" des données préalablement chiffrées est également l'un des aspects traités par des deux des dispositions introduites par amendement après le 11 septembre dans le projet de loi LSQ.

Là encore, c'est en prévision de la future (mais toujours repoussée) loi sur la société de l'information (LSI, destinée à transposer la plupart des dispositions de la directive sur le commerce électronique du 8 juin 2000) qu'avait été rédigé – avec peine – plusieurs dispositions relative à la cryptographie. Mais l'urgence de la lutte anti-terroriste et de l'affichage politique d'une riposte s'imposant, ces dispositions ont trouvé place dans la LSQ et viennent, pour l'une d'entre elle, compléter le code de procédure pénale, et pour la seconde, compléter la loi du 10 juillet 1991 relative au secret des télécommunications et aux interceptions.

3.1. Une conséquence indirecte de la libéralisation progressive du régime de la cryptologie

Pour comprendre le contexte de ces deux dispositions, il faut se souvenir que le gouvernement français a renoncé, en 1999 à poursuivre une politique de prohibition indirecte de l'usage des moyens de chiffrement et a, notamment, cessé de soumettre à autorisation (remplacée par une simple déclaration) le commerce et l'utilisation des moyens de chiffrement utilisant des clés d'une longueur inférieure ou égale à 128 bits [14]. Et l'on annonce, depuis longtemps, que cette libéralisation devrait aboutir à un régime de quasi-liberté prévue dans le projet de loi LSI.

Dans ces conditions, les services gouvernementaux se préparent à une situation dans laquelle un volume croissant de communications électroniques (notamment de courriers électroniques) susceptibles d'intéresser les enquêtes des services de renseignement et de la police judiciaire va être chiffrée avec des moyens techniques de haut niveau, difficiles à décrypter sans connaître la clé de chiffrement employée. Anticipant donc depuis plusieurs années une possible défaite des moyens d'investigation gouvernementaux (et notamment des

[14] Décret n°99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation ; Décret n°99-200 du 17 mars 1999 les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable (*J.O.R.F.* du 19 mars 1999, pp. 4050-4053). Pour une synthèse de l'évolution de la législation et de la politique française depuis 1990, cf. Bertrand Warusfel, " Dix ans de réglementation de la cryptologie en France : du contrôle étatique à la liberté concédée", *Annuaire Français de Relations Internationales*, 2000, n° 1.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

moyens d'interception, qui ne seraient plus efficaces dès lors que les communications interceptées seraient rendues intelligibles par le chiffrement) face aux nouvelles technologies numériques et mathématiques, ces services ont su convaincre les autorités gouvernementales de la nécessité de mettre en place des moyens palliatifs.

Le nouvel chapitre du code de procédure pénale consacré à "la mise au clair des données chiffrées nécessaires à la manifestation de la vérité" et le nouvel article 11-1 introduit dans la loi du 10 juillet 1991 par la LSQ illustre les deux types de réplique que l'appareil de sécurité nationale entend déployer pour faire face à une possible croissance de l'usage des moyens cryptologiques par les délinquants : la voie technique du décryptement et la voie procédurale de l'obligation de livrer les clés.

3.2. Le recours aux moyens spéciaux pour le décryptement des données chiffrées

Le nouveau chapitre du code de procédure pénale créé par la LSQ concerne *"la mise au clair des données chiffrées nécessaires à la manifestation de la vérité"* (nouveaux articles 230-1 à 230-5 CPP). En termes plus simples, cela concerne l'organisation du "décryptement" des messages chiffrés (c'est-à-dire, l'emploi de moyens techniques sophistiqués pour tenter de retrouver le contenu "clair" du message d'origine, sans avoir connaissance de la clé de chiffrement qui a été utilisée [15]). Or, la particularité du fonctionnement de nos services de sécurité (comme de ceux de la plupart des États contemporains) tient au fait que seuls les services de renseignement disposent réellement de compétences et de moyens techniques spécialisés pour se livrer à ce type de travail. En France, c'est principalement la Direction technique de la Direction générale de la sécurité extérieure (DGSE) qui a en charge ce que l'on appelle, dans la terminologie officielle, le "chiffre offensif". C'est la raison pour laquelle, le nouvel article 230-1 CPP parle de recourir *"aux moyens de l'État soumis au secret de la défense nationale"* . Par là, le législateur désigne indirectement un mystérieux "centre technique d'assistance" (selon les travaux parlementaires) qui mettra en œuvre ces moyens discrets mais il indique aussi une particularité juridique qui va exercer ses effets sur la procédure de mise au clair elle-même.

En effet, il n'est pas usuel ni facile de faire travailler ensemble et dans un même but des services travaillant dans le cadre de la procédure pénale (avec toutes ses exigences en termes de contrôle et de respect des droits de la défense et du contradictoire) et une entité dont l'activité est soumis à un secret si strict qu'il s'oppose même encore aujourd'hui aux juridictions pénales [16]. C'est pourquoi, le nouveau texte a prévu un interface chargé de faire à la fois le relais et le "tampon" entre la demande des autorités judiciaires souhaitant disposer du décryptement d'un message ou d'un fichier informatique chiffré et la prise en charge de ce travail par les moyens spécialisés des services spéciaux. Ce sera le rôle – parmi d'autres – du nouvel office de police judiciaire spécialisé dans les technologies de l'information, l'Office

[15] C'est également ce que communément on appelle "casser" un message chiffré.

[16] Sur l'ensemble du régime juridique du secret de défense, et en particulier sur l'opposition entre secret de défense et procédures judiciaires, cf. notre ouvrage, Bertrand Warusfel, *Contre-espionnage et protection du secret – Histoire, droit et organisation de la sécurité nationale en France*, Lavauzelle, 2000.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

central de lutte contre la criminalité liée aux technologies de l'information et de la communication [17].

En quelque sorte, l'organisme technique concerné jouera dans ce processus le rôle habituellement dévolu aux experts mandatés par la justice pour concourir à la manifestation de la vérité. Mais avec une limite cependant et qui n'est pas mince : à la différence d'une expertise dont l'expert rend compte directement et complètement et qui est communiquée de manière contradictoire et versée au dossier, seul le résultat du décryptement sera tranmis, accompagné *"d'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis"* ainsi qu'éventuellement et *"sous réserve des obligations découlant du secret de la défense nationale"* des *"indications techniques utiles à la compréhension et à leur exploitation"* (art. 230-3).

On voit donc que le versement de tels décryptements au dossier d'une instruction criminelle donnera souvent lieu à des contestations et qu'il ne sera pas aisé aux magistrats de justifier, sans pouvoir faire témoigner les techniciens concernés, la foi qu'ils apporteront à ces éléments de preuve issus de communications électroniques et de traitements numériques complexes. Tout au plus peut-on constater, avec faveur, que le dispositif imaginé s'efforce de rester simple et qu'il est précisé que – toujours *"sans préjudice des obligations découlant du secret de la défense nationale"* - *"les agents requis en application des dispositions du présent chapitre sont tenus d'apporter leur concours à la justice."* (article 230-5).

3.3. L'obligation de livraison des clés de déchiffrement

Faute de devoir toujours compter sur les hypothétiques apports de la technique, la LSQ a également suivi les prescriptions du Conseil de l'Europe et choisi de renforcer les moyens juridiques offerts à l'autorité judiciaire et aux services d'investigation pour se faire remettre par quiconque en est possesseur les clés permettant le déchiffrement des données chiffrées dont le contenu peut concourir à la manifestation de la vérité dans le cadre d'une enquête pénale.

Deux cas peuvent, en effet, se présenter. Le plus favorable est celui où un prestataire extérieur identifié se trouvera en possession des clés nécessaires au déchiffrement des données concernées. Ce cas pourra se produire, notamment, à chaque fois que la personne ayant effectué le chiffrement des données aura eu recours à un *"prestataire de services de cryptologie"* au sens de la législation française sur la cryptologie [18]. Dès lors, le nouvel article 11-1 qu'introduit la LSQ (par son article 31) dans la loi du 10 juillet 1991, prévoit simplement que ces prestataires assurant un service de confidentialité (c'est-à-dire le chiffrement) *" sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en oeuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces*

[17] Décret n°2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, *J.O.R.F.* n°113, 16 Mai 2000.
[18] Article 28 de la loi n° 90-1170 du 29 décembre 1990 prévoit que sont soumis à contrôle les moyens et les prestations de cryptologie.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22

réquisitions." Et le non-respect de cette obligation est sanctionnée pénalement (par une peine de deux ans d'emprisonnement et de 30.000 € d'amende).

L'autre cas est celui où les clés de déchiffrement sont détenus par la personne ayant effectué elle-même le chiffrement ou par d'autres personnes tierces n'ayant pas la qualité de prestataire de services de cryptologie. Pour faire pression sur ces détenteurs, la LSQ a introduit dans le code pénal un nouvel article 434-15-2 punissant de trois ans d'emprisonnement et de 45.000 € d'amende *"le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités"*. Et les peines sont aggravées lorsque la commission d'un crime ou d'un délit aurait pu être évité ou leurs conséquences amoindries par une telle remise.

En maniant ainsi la riposte technique (mise en œuvre dans un cadre reconnu des moyens techniques spéciaux) et les contraintes juridiques (pour forcer à la remise des clés), les services de l'État en charge de la sécurité nationale et le législateur ont voulu mettre en œuvre ce que recommandait le Conseil de l'Europe en 1995, en disant – comme déjà mentionné plus haut, qu'il conviendrait de prendre des mesures pour *"minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales"*.

Reste maintenant à évaluer l'efficacité qu'aura un tel dispositif complexe et sans doute trop rapidement voté pour être parfaitement exempt de lacunes juridiques et pratiques. Reste aussi – et surtout – à s'interroger sur la compatibilité de toutes ces nouvelles orientations "sécuritaires" avec le nécessaire respect des libertés individuelles et de la vie privée des citoyens. On sait qu'aux Etats-Unis, toutes les mesures pour encadrer trop strictement l'usage des moyens de communication numériques (et y compris, les moyens de chiffrement) au nom de la sécurité (même nationale) ont toujours été (en tout cas, au moins jusqu'au 11 septembre 2001) fort mal admises. On se rend compte également qu'un excès de zèle en matière de sécurité technologique pourrait être néfaste, y compris à la sécurité quotidienne des citoyens [19]. Le débat ne fait donc que commencer, même si l'on peut se féliciter que, refusant de trop céder à la panique ou à la démagogie, le législateur français se soit limité dans ces amendements "technologiques" à la LSQ à transposer les exigences qui sont désormais les siennes du fait de l'adoption de la Convention sur la cybercriminalité.

Bertrand WARUSFEL

[19] Cf. l'article de Franc Leprévost dans ce même numéro.

Article publié dans le numéro 2002/1
de la Revue *DROIT & DÉFENSE*, pp. 17-22