Projet envoyé en consultation

Département fédéral de justice et police

Approbation et mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité

Avant-projet et rapport explicatif

Office fédéral de la justice
Berne, mars 2009

Condensé

Le Conseil fédéral entend proposer à l'Assemblée fédérale d'approuver la Convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité. Celle-ci, entrée en vigueur le 1er juillet 2004, est la première convention internationale, et à ce jour la seule, à traiter de cybercriminalité. Les Etats Parties s'y engagent à adapter leur législation aux défis posés par les nouvelles technologies de l'information. La Suisse remplit déjà largement les exigences de la Convention. Seules de petites adaptations du code pénal et de la loi sur l'entraide pénale internationale ainsi que quelques réserves et déclarations sont nécessaires.

La première partie de la Convention contient des dispositions pénales matérielles ; il s'agit d'harmoniser le droit pénal des Etats. La deuxième partie contient des règles de procédure pénale concernant essentiellement l'administration et la conservation des preuves électroniques lors des enquêtes pénales. Enfin, la Convention vise à mettre en place un régime rapide et efficace de coopération pénale entre les Etats Parties.

La Suisse a signé la Convention le 23 novembre 2001. Le 27 février 2008, le Conseil fédéral a proposé d'accepter la motion Glanzmann-Hunkeler (07.3629) qui demandait qu'elle soit ratifiée.

Le droit pénal matériel suisse, dont les dispositions sur les infractions dans le domaine informatique sont entrées en vigueur le 1er janvier 1995, satisfait manifestement en majeure partie aux exigences de la Convention. Il faut seulement modifier la définition de l'accès indu à un système informatique (ce que l'on appelle le « piratage informatique », art. 143bis du code pénal), en pénalisant des actes commis antérieurement au piratage lui-même, c'est-à-dire le fait de mettre en circulation ou de rendre accessible un mot de passe ou un programme en sachant qu'il doit être utilisé pour s'introduire sans droit dans un système informatique. Nous proposons aussi, bien que la Convention ne l'exige pas, de supprimer le critère du dessein d'enrichissement dans cet article, car il a fait l'objet de nombreuses critiques des auteurs de doctrine.

Pour ce qui est des règles de procédure, le code de procédure pénale adopté par le Parlement le 5 octobre 2007, et dont l'entrée en vigueur est prévue pour le 1er janvier 2011, répond manifestement aux exigences de la Convention. Il permettra de mettre en œuvre les dispositions de procédure de cette dernière de façon uniforme dans toute la Suisse.

Dans le domaine de la coopération internationale, une modification (nouvel art. 18b de la loi sur l'entraide pénale internationale) est également nécessaire à la mise en œuvre des art. 30 et 33 de la Convention. L'autorité d'exécution suisse est ainsi autorisée à divulguer les données relatives au trafic informatique avant la clôture de la procédure. Cette possibilité trouve sa justification dans le caractère éphémère des données informatiques. Elle est toutefois limitée à deux situations particulières et est accompagnée de restrictions garantissant que les droits de la personne touchée restent protégés de manière adéquate.

Table des matières

1 Les grandes lignes de la Convention

1.1 Contexte et genèse

L'essor des technologies informatiques a transformé le visage de notre société. Il a simplifié les actes et les tâches les plus quotidiens du domaine de la communication. Un individu peut transmettre instantanément des données saisies ou conservées en un lieu quelconque à un destinataire précis ou bien à un ensemble de personnes ou d'institutions n'importe où dans le monde. Il est possible de donner accès à des informations enregistrées dans un système informatique à un cercle de personnes relativement indéterminé, qui peuvent les chercher de manière ciblée et les télécharger.

Si cette évolution a des retombées positives sur l'économie, la politique et la société, elle comporte aussi des aspects plus inquiétants. Ce même progrès technologique qui offre de grands avantages à un vaste partie de la population permet de commettre de nouveaux types d'infractions ou offre de nouveaux moyens (numériques) pour commettre des infractions « classiques ». La fraude sur Internet, la diffusion de contenus illégaux et l'apologie de la haine, de la violence et de la terreur ne sont que quelques exemples des nouvelles dérives qui préoccupent depuis un certain temps l'opinion publique et les organisations nationales et internationales.

En avril 1997, un groupe d'experts institué par le Comité des ministres du Conseil de l'Europe a mis en chantier un projet de Convention sur la cybercriminalité. Outre les Etats membres, les Etats-Unis, le Canada, l'Afrique du Sud et le Japon ont pris part aux négociations. Les travaux ont duré jusqu'au printemps 2001. Une fois adopté par les organes compétents du Conseil de l'Europe, le texte a été ouvert à la signature le 23 novembre 2001 à Budapest. La Suisse l'a signé à cette occasion. La Convention est entrée en vigueur le 1er juillet 2004 et a été ratifiée à ce jour par 23 Etats[1].

1.2 Aperçu du contenu de l'accord

La Convention du Conseil de l'Europe sur la cybercriminalité est la première Convention internationale, et à ce jour la seule, à traiter de cybercriminalité. Les Etats Parties s'y engagent à adapter leur droit pénal matériel, leur procédure pénale et leurs dispositions en matière d'entraide judiciaire aux défis posés par les nouvelles technologies de l'information.

La Convention contient en premier lieu des dispositions pénales matérielles qui visent à harmoniser le droit pénal des Etats. Les Etats Parties s'engagent à sanctionner notamment la fraude et la falsification informatiques, le vol de données et l'introduction illicite dans un système informatique protégé (art. 2 à 8). Ils doivent punir toute forme de pornographie enfantine sur Internet (art. 9). Les atteintes à la propriété intellectuelle commises par voie électronique sont également visées

[1] Etat: décembre. On trouvera le texte de la Convention et son rapport explicatif (ci-après « rapp. expl. ») à l'adresse http://Conventions.coe.int/Treaty/FR/v3DefaultFRE.asp (STE n° 185).

(art. 10). Enfin, les Etats Parties doivent instaurer une responsabilité des personnes morales pour les infractions visées par la Convention (art. 12).

Dans une deuxième partie, la Convention prévoit des règles de procédure pénale relatives à l'administration et à la conservation des preuves sous forme de données informatiques au cours de l'instruction (art. 16 à 21). Les données informatiques peuvent être modifiées à distance en l'espace de quelques secondes, si bien qu'il importe d'assurer leur préservation lorsqu'elles doivent être utilisées dans une instruction et d'éviter leur falsification ou leur destruction en cours de procédure. Les autorités d'instruction doivent donc pouvoir y accéder rapidement et les conserver sans tarder.

Dans une troisième partie, la Convention traite de la coopération internationale en matière pénale (entraide judiciaire, extradition, mesures provisoires, etc. ; art. 23 à 35). Elle a pour but de mettre en place un régime rapide et efficace de coopération et précise que celle-ci doit être réalisée dans la mesure la plus large possible.

1.3 Appréciation de la Convention

La Convention du Conseil de l'Europe sur la cybercriminalité, élaborée en réaction aux nouveaux défis que les technologies de l'information posent aux Etats et à la communauté internationale[2], reconnaît la nécessité de combattre et de prévenir non seulement à l'intérieur des frontières nationales mais aussi au niveau international cette délinquance qui s'exerce à l'échelle du monde. On ne peut que saluer l'ambition qu'a la Convention d'harmoniser les législations nationales des Etats d'Europe et au-delà et de renforcer la coopération internationale. Des effets positifs se dessinent déjà dans le cadre de la mise en œuvre au niveau national. Plusieurs Etats ont adapté leur législation, prenant la Convention comme standard et s'inspirant du savoir acquis par le Conseil de l'Europe.

Il ne faut pas pour autant surestimer l'importance de la Convention aujourd'hui. De nombreux pays ont une infrastructure encore insuffisante pour lutter contre la cybercriminalité (équipement technique et capacités des autorités, possibilités de surveillance). Quant aux Etats membres qui possèdent une batterie d'instruments efficaces contre les cyber-infractions, les conséquences pratiques de la Convention y sont jugées minimes, notamment faute de mécanisme de monitoring et en raison des échanges encore assez faibles entre les Etats Parties.

2 Les dispositions de la Convention et leur relation avec la législation suisse

2.1 Chapitre I: Terminologie

2.1.1 Art. 1 - Définitions

L'art. 1 décrit les notions de « système informatique », « données informatiques », « fournisseur de services » et « données relatives au trafic ». Ces dernières portent tout particulièrement sur l'expéditeur et le destinataire, la date, la durée, la taille et l'itinéraire de la communication. La terminologie de la Convention s'écarte sur ce point de celle de l'art. 2, let. g, de l'ordonnance du 31 octobre 2001 sur la

2 Voir ch. 1.1.

surveillance de la correspondance par poste et télécommunication[3], où il est question des données que les fournisseurs de services enregistrent comme justificatif des communications. La partie de la Convention relative à la procédure[4] revient plus en détail sur ce terme de « données relatives au trafic ». Pour le reste, les définitions de la Convention ne diffèrent guère, sur le plan pratique, de celles que l'on utilise en Suisse.

2.2 Chapitre II: Mesures à prendre au niveau national

2.2.1 Art. 2 – Accès illégal

L'art. 2 de la Convention vise une criminalisation du piratage (« *hacking* ») uniforme au niveau international. Doit être punissable pénalement toute personne qui accède intentionnellement et sans droit à l'ensemble ou à une partie d'un système informatique. Les Etats Parties peuvent remettre une déclaration[5] selon laquelle ils exigent qu'il y ait aussi punissabilité en cas de violation des mesures de sécurité, en cas d'intention d'obtenir des données informatiques ou autre intention délictueuse ou en cas de relation avec un système informatique connecté à un autre système informatique.

L' art. 143bis du code pénal (CP)[6] couvre les accès indus à des données par des intrus (les « *hackers* » ou pirates): sera punie toute personne qui, sans dessein d'enrichissement, se sera introduite sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part.

L'art. 2 de la Convention est couvert pour l'essentiel par l'art. 143bis CP. La différence réside dans l'exigence que le système soit protégé. Il est possible de ne pas modifier l'article du CP : la Suisse peut remettre une déclaration selon laquelle il faut qu'un système de protection de l'accès ait été contourné[7]. La remise d'autres déclarations relatives à l'art. 2 de la Convention ne semble pas nécessaire. Cet article ne requiert par ailleurs aucune modification de loi.

La formulation de l'art. 143bis CP (« sans dessein d'enrichissement ») a souvent été critiquée par la doctrine[8], qui lui reproche de sanctionner des personnes agissant par curiosité, qui ne seraient pas punissables, dans certaines circonstances, si elles avaient pour but de s'enrichir. C'est oublier que celui qui pénètre dans un ordinateur avec un dessein d'enrichissement veut généralement se procurer des données, c'est-à-dire les garder en vue d'une utilisation future par soi-même ou par un tiers[9], cas de figure soumis à une peine plus élevée par l'art. 143 CP[10]. S'il ne soustrait pas des

3 OSCPT, RS **780.11**.
4 Art. 14 ss.
5 Art. 40 de la Convention.
6 RS **311**.
7 Une déclaration similaire a été remise par quelques Etats membres à propos de l'art. 2; cf. la liste des déclarations des Parties à l'adresse suivante : http://conventions.coe.int/. La possibilité de remettre des déclarations et des réserves a été expressément prévue comme partie intégrante à la Convention lors de l'élaboration de celle-ci (cf. ch. 49 et 50 du rapp. expl., lien disponible sous note 1).
8 Ph. Weissenberger, in: Basler Kommentar, Strafrecht II, n. 25 ad art. 143bis, Bâle 2007; S. Trechsel *et al.*, Schweizerisches Strafgesetzbuch, Praxiskommentar, St-Gall 2008, n. 10 ad art. 143bis.
9 Cette opinion a également été exprimée lors des débats parlementaires, cf. Bull. Sténo. du Conseil national, 1993, p. 935 ss.
10 Soustraction de données.

données, il essaie de tirer un avantage de son action, par exemple d'inciter un tiers à lui fournir une prestation simplement en entrant dans son ordinateur ou en le menaçant d'endommager ses données. Or ce fait est puni par les dispositions pénales protégeant le patrimoine ou la liberté[11]. Il n'en est pas moins vrai que l'exclusion du dessein d'enrichissement dans la définition de l'infraction à l'art. 143bis CP est irritante et que l'application rigoureuse de ce critère n'était pas dans les intentions du législateur. L'autorité qui applique le droit se voit confrontée à la question du motif de cette restriction, à laquelle il est malaisé de répondre, et doit déterminer, lorsque l'auteur avait le dessein de s'enrichir et commettait donc un acte plus répréhensible, sur quelle base fonder sa punissabilité[12]. De plus, le critère de l'absence de dessein d'enrichissement entre forcément en conflit avec la volonté exprimée à l'art. 6 de la Convention de punir les personnes agissant en amont du piratage[13], si bien qu'il nous paraît indiqué de sanctionner aussi la diffusion d'un mot de passe *avec* un dessein d'enrichissement, afin d'éviter toute lacune de la législation pénale.

Nous proposons donc de saisir l'occasion de la mise en œuvre de la Convention sur la cybercriminalité pour supprimer le critère de l'absence de dessein d'enrichissement à l'art. 143bis CP (pour la formulation, voir le commentaire de l'art. 6 de la Convention[14]). La définition du piratage (associé pour l'heure à un acte gratuit) sera étendue aux actes commis dans un dessein d'enrichissement. Cela explicitera la volonté du législateur de punir toute intrusion dans un système dans un dessein d'enrichissement tout en mettant fin aux critiques. On écartera aussi le risque de lacune à l'art. 143bis, qui, bien que minime, n'était pas totalement à exclure. Une personne qui s'introduit dans un système informatique protégé dans un dessein d'enrichissement et en soustrait des données continuera de se rendre coupable de soustraction de données (art. 143 CP), ce qui consumera pénalement l'art. 143bis.

2.2.2 Art. 3 – Interception illégale

Conformément à l'art. 3 de la Convention, doit être punissable quiconque intercepte intentionnellement et sans droit, à l'aide de moyens techniques, des données informatiques lors de transmissions non publiques, y compris les émissions électromagnétiques. L'interception comprend l'écoute, la surveillance, l'obtention et l'enregistrement des données[15]. Etant donné la similitude de situation avec l'art. 2 de la Convention, les Etats Parties ont là aussi la possibilité, au moyen d'une déclaration, de lier la pénalisation à d'autres conditions, à savoir la connexion avec un autre système informatique ou l'existence d'une intention délictueuse.

Le droit pénal suisse ne possède pas de réglementation correspondant à l'art. 3 de la Convention, mais plusieurs normes pénales assurent une protection partielle. L'art. 321ter CP protège le secret des postes et des télécommunications, dont la violation est punie d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Son champ d'application se limite toutefois aux fonctionnaires et à

11 Par ex. l'art. 156 (Extorsion et chantage) ou 181 (Contrainte) CP.
12 Dans le projet du Conseil fédéral, les art. 143 et 143bis formaient une seule et même disposition (cf. FF **1991** II 977). L'acte commis sans dessein d'enrichissement était une variante privilégiée de l'infraction principale.
13 Voir le commentaire de l'art. 6 de la Convention.
14 Voir ch. 2.2.5.
15 Voir ch. 53 du rapp. expl. (lien disponible sous note 1).

des personnes occupant une position ou une fonction particulière. Quant à la punissabilité conformément à l'art. 143bis CP (piratage), elle est limitée à l'intrusion dans un système informatique. Cette disposition ne protège donc pas les installations de transmission elles-mêmes, à moins que celles-ci ne constituent des systèmes informatiques au sens de la norme pénale[16].

Conformément à l'art. 143 CP[17], est punissable celui qui se procure, dans un dessein d'enrichissement illégitime, des données enregistrées électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part. Se procurer au sens de la loi signifie obtenir le pouvoir de disposer des données; il n'est pas nécessaire que l'auteur de cet acte enregistre les informations sur un support de données qui lui appartient. Il suffit qu'il puisse les mettre en œuvre pour ses propres besoins en dehors de l'ordinateur[18]. La réception ou l'écoute d'une « émission » électromagnétique, produite par un système informatique ou par une installation de transmission de données, est également visée[19].

En exigeant que le système informatique soit spécialement protégé, le législateur limite le champ d'application de l'art. 143 CP aux cas dans lesquels la personne ayant légalement accès aux données manifeste sa volonté d'empêcher que des tiers n'accèdent à ses données ou de restreindre cet accès. Mis à part le verrouillage de locaux et d'armoires, par exemple, l'utilisation d'un chiffrement, de codes d'accès, de clefs biométriques ou de mots de passe est également une mesure de sécurité possible. La protection doit être *habituellement suffisante* pour empêcher un accès illégal[20]. Il n'est pas nécessaire, par exemple, que des mesures de protection spécifiques, allant au-delà d'une protection contre les virus et les accès illicites habituelle sur le marché[21], aient été prises. La norme pénale ne s'applique pas, par contre, à une attaque contre des données non protégées ou à leur utilisation illicite[22].

L'art. 3 de la Convention ne porte toutefois que sur les *transmissions* de données informatiques. Lorsqu'il y a transmission de données, les exigences de protection sont en général réduites[23]. On ne peut pas exiger en principe que des mesures de protection par chiffrement, par exemple, aient été prises pour que l'art. 143 CP s'applique. Cet article correspond donc à la disposition de l'art. 3 de la Convention. Il n'y a pas lieu, comme nous l'avons montré, de prévoir des exigences plus strictes pour la protection des transmissions de données non publiques. La norme pénale prévoit cependant que l'action doit avoir été commis dans un dessein d'enrichissement illégitime. Il faudra donc émettre une déclaration sur ce point.

Selon le rapport explicatif relatif à la Convention[24], le flux d'informations à l'intérieur d'un système informatique doit aussi être considéré comme une

16 N. Schmid, Computerkriminalität, Zurich 1994, § 5 n. 16.
17 Soustraction de données.
18 Mais éventuellement sans les employer véritablement (N. Schmid, *loc. cit.*, § 4 n. 40 s).
19 N. Schmid, *op. cit.*, § 4 n. 30 et n. 51.
20 Cf. Weissenberger, *op. cit.*, n. 18 *ad* art. 143.
21 Par ex. dans le cas de l'intrusion d'un « cheval de Troie » ; cf. le jugement du 13 novembre 2007 de la 2^{e} chambre pénale du tribunal cantonal de Berne, SK 2007/187.
22 Par ex. dans le cas d'un ordinateur utilisé en commun ou de l'utilisation illicite de données par une personne à qui elles ont été confiées.
23 Cf. Chr. Schwarzenegger, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, *in* : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002, p. 305 ss.
24 Voir ch. 55 du rapp. expl. (lien disponible sous note 1).

transmission de données au sens de l'art. 3 de la Convention. Cela inclut les transmissions sans fil, toujours plus nombreuses, entre l'ordinateur et les appareils périphériques (imprimante, clavier, écran, etc.). Ces données sont relativement faciles à intercepter pour ceux qui disposent de l'équipement et des connaissances nécessaires, mais on considère néanmoins qu'elles sont spécialement protégées contre un accès indu, en raison de leur caractère non public, de leur portée généralement faible et du fait que l'auteur, agissant sciemment, doit prendre des dispositions considérables pour y avoir accès. L'art. 143 CP est donc aussi applicable dans ce cas. Il n'est pas nécessaire d'adapter la loi sur ce point en sus de la déclaration mentionnée ci-avant.

2.2.3 Art. 4 – Atteinte à l'intégrité des données

Selon cette disposition, doit être punissable le fait d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données sans droit et de manière intentionnelle. Un Etat Partie peut, par le biais d'une réserve[25], déclarer comme condition de la punissabilité le fait que le comportement en question entraîne des dommages sérieux.

Conformément à l'art. 144bis CP (Détérioration de données), celui qui sans droit modifie, efface ou met hors d'usage des données enregistrées ou transmises électroniquement ou sur un mode similaire est puni sur plainte. Par « mettre hors d'usage », on vise le cas d'une personne qui empêche l'ayant droit de faire usage de ses données, même avec un effet provisoire[26]. Le fait de « supprimer » au sens de la Convention est couvert par le droit en vigueur. Quant au fait d'endommager ou de détériorer, il est ouvert par les termes de « modifier » et de « mettre hors d'usage ». La punissabilité requise est garantie par l'art. 144bis CP.

2.2.4 Art. 5 – Atteinte à l'intégrité du système

Conformément à l'art. 5 de la Convention, se rend punissable quiconque entrave gravement, de manière intentionnelle et sans droit, le fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques. Il y a notamment entrave grave en cas d'envoi de données dont la forme, le volume ou la fréquence restreint considérablement le fonctionnement d'un système informatique[27]. Même lorsqu'il est perçu comme gênant, l'envoi en masse de courrier électronique non sollicité[28] n'est pas couvert par cette disposition[29].

25 Art. 42 de la Convention. Quelques Etats ont déjà fait usage de cette possibilité, voir http://conventions.coe.int/.

26 N. Schmid, *loc. cit.*, n. 29 *ad* art. 144bis; Stratenwerth, *loc. cit.*, n. 49 *ad* § 14; voir aussi ch. 61 du rapp. expl. (lien disponible sous note 1).

27 Blocage ou paralysie intentionnels; voir ch. 67 du rapp. expl.

28 « *Spamming* ». Une norme pénale à ce sujet est entrée en vigueur en droit suisse le 1er avril 2007 (art. 3, let. o, de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale, RS **241**).

29 Voir ch. 69 du rapp. expl. (lien disponible sous note 1).

Ces faits sont couverts par l'infraction de la détérioration de données définie par l'art. 144bis CP qui punit aussi la mise hors d'usage temporaire de données et le blocage de l'accès à des données pendant un laps de temps considérable[30].

2.2.5 Art. 6 – Abus de dispositifs

2.2.5.1 Exigences de la Convention

Selon l'art. 6 de la Convention, doivent être déclarées punissables, lorsqu'elles sont commises intentionnellement et sans droit, la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou autres formes de mise à disposition de dispositifs, logiciels[31], codes d'accès ou mots de passe utilisés pour permettre la commission de l'une des infractions établies conformément aux articles précédents[32]. L'intention doit se référer, outre à l'acte lui-même, à la commission des infractions visées aux art. 2 à 5[33]. En d'autres termes, celui qui vend ou transmet un des éléments cités doit être pleinement conscient qu'il sera ultérieurement utilisé illégalement et agir dans cette intention. Doit également être déclarée punissable la possession d'un de ces éléments dans l'intention qu'il soit utilisé afin de commettre l'une des infractions visées[34].

La Convention accorde aux Etats Parties différentes possibilités de déposer des réserves et d'adopter des normes nationales divergentes. Ainsi la possession peut n'être punissable que si elle porte sur un nombre minimum de ces éléments. Le par. 3 prévoit la possibilité d'une réserve générale[35], selon laquelle seules la vente, la distribution ou la mise à disposition de mots de passe, de codes d'accès ou autres données similaires sont pénalisées.

2.2.5.2 Modification de l'art. 143bis CP

Conformément à l'art. 144bis, ch. 2, CP, est punissable quiconque a fabriqué, importé, mis en circulation, promu, offert ou d'une quelconque manière rendu accessibles des logiciels dont il savait ou devait présumer qu'ils devaient être utilisés dans le but de modifier ou de détériorer illégalement des données, ou qui a fourni des indications en vue de leur fabrication. Il s'agit ici de la norme concernant les virus informatiques, qui permet de punir les actes préparatoires visant une détérioration des données. Il y a également infraction en cas de dol éventuel, lorsque la détérioration des données est commise par un tiers[36].

L'art. 6 de la Convention est couvert, dans sa substance, par l'article pénal cité. En outre, notamment dans les cas où il ne s'agit ni de modification ni d'effacement de données, et où des programmes ne sont pas mis en circulation, les dispositions relatives à la complicité et à la tentative[37] sont applicables, en relation avec les art. 143 et 143bis CP.

En cas de possession ou de production de dispositifs, de programmes ou autres éléments avec intention de les utiliser illégalement, on peut admettre qu'il y a

30 Par ex. par l'envoi d'importantes masses de données modifiées sur des serveurs qui s'en sont trouvés paralysés (cf. Weissenberger, *loc. cit.*, n. 23 *ad* art. 144bis).
31 Par ex. les programmes-virus; voir ch. 72 du rapp. expl. (lien disponible sous note 1).
32 Art. 6, par. 1, let. a.
33 Art. 6, par. 1, let. a, *in fine*.
34 Art. 6, par. 1, let. b.
35 Art. 42 de la Convention.
36 Cf. ATF 129 IV 230.
37 Art. 22 et 25 CP.

tentative, dans certaines circonstances, et donc punissabilité, compte tenu de la doctrine et de la jurisprudence actuelles relatives à la tentative (inachevée) punissable en droit pénal conformément à l'art. 22, al. 1, CP[38]. Si l'on peut prouver à satisfaction de droit que le producteur ou le propriétaire a eu cette intention (le texte de la Convention part de cette hypothèse), on peut considérer que le coupable a manifesté son intention au sens du dépassement du seuil de la tentative (mais n'a pas encore tout fait pour réaliser la consommation de l'infraction).

Est puni à titre de complice quiconque prête intentionnellement assistance à l'auteur d'un crime ou d'un délit, donc soutient l'acte intentionnel d'autrui à titre subordonné[39]. Le complice n'a besoin de connaître ni la victime, ni l'auteur, ni les modalités précises de l'acte[40]. L'importation, l'obtention et la diffusion délibérées de dispositifs, mots de passe et programmes en toute conscience du fait qu'ils seront utilisés pour commettre des infractions et dans l'intention qu'ils le soient, peuvent donc constituer une infraction au titre de complicité, en relation avec les art. 143, 143bis et 144bis. Il convient toutefois de noter à ce propos qu'outre la tentative de complicité, l'assistance concernant un acte principal qui n'a pas (encore) fait l'objet d'une tentative n'est pas punissable. De même que nous l'avons mentionné plus haut, il faut qu'il y ait un lien et une proximité matérielle et temporelle avec une infraction concrète.

Par contre, la personne possédant ou produisant un tel dispositif dans l'idée que celui-ci soit éventuellement, à un moment ultérieur indéterminé, utilisé par une tierce personne à des fins délictueuses, n'est pas punissable, en vertu du principe du caractère accessoire effectif[41]; il n'y a pas la corrélation requise avec un acte principal pour lequel au moins des plans avaient été établis. Dans le cas où une personne communique un code d'accès[42] dans l'intention de le voir utilisé pour la commission d'une infraction mais où celle-ci n'a pas commencé, il n'y a pas comportement punissable en vertu du droit suisse. Or la Convention requiert la punissabilité dans ce cas[43]. Il conviendrait d'envisager une modification de l'art. 143bis couvrant la diffusion illégale des codes d'accès ou autres données similaires et incriminant donc certains actes préparatoires du piratage[44], comme à l'art. 144bis, ch. 2, CP. Elle devrait prendre la forme suivante :

> [1]*Quiconque, ~~sans dessein d'enrichissement~~, s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*
>
> [2]***Quiconque met en circulation ou rend accessible un mot de passe, un programme ou toute autre donnée dont il sait ou doit présumer qu'ils doivent être utilisés dans le but mentionné à l'al. 1*** *est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.*

38 Cf. ATF 114 IV 114; 119 IV 227; S. Trechsel / P. Noll, Schweizerisches Strafrecht, AT I, Zurich 1998, p. 174 ss.
39 Cf. S. Trechsel, Kurzkommentar, Zurich 1997, n. 1 *ad* art. 25.
40 Forster, in: Basler Kommentar, StGB I, 2003, n. 19 *ad* art. 25.
41 Cf. S. Trechsel, *op. cit.*, n. 21, Vor Art. 24.
42 Et non un programme au sens de la loi.
43 Cf. art. 6, par. 3.
44 Cf. Schmid, *loc. cit.*, n. 31 *ad* art. 143bis.

La nouvelle infraction – divulguer un mot de passe, un programme ou toute autre donnée – sera poursuivie d'office. Contrairement à l'intrusion elle-même, cet acte ne peut en général pas être assigné à une cible concrète, donc relié à une personne habilitée à porter plainte. Citons comme exemple la divulgation sur Internet de données permettant de casser les protections similaires d'un grand nombre d'ordinateurs.

Nous proposons de supprimer la référence au dessein d'enrichissement (cf. le commentaire de l'art. 3 de la Convention[45]) afin de punir de manière plus cohérente les actes préparatoires, sans avoir à faire de distinction selon qu'il y a ou non dessein d'enrichissement.

Le complément proposé se rapproche des exigences de la Convention. Il restreint légèrement, mais dans une mesure que nous considérons comme proportionnée, le champ des infractions possibles par rapport à la définition actuelle de la « détérioration de données »[46]. Sera sanctionné le fait de *rendre accessible* et de *mettre en circulation* des données, deux notions qui peuvent être interprétées très largement et qui se recoupent en partie.

Par ailleurs, il semble indiqué d'émettre une réserve excluant la punissabilité de la possession, de l'importation et de la production des données, à moins que ces actes ne visent la détérioration ou la modification de données ou ne puissent être qualifiés de complicité ou de tentative punissable d'un autre acte[47].

2.2.6 Art. 7 – Falsification informatique

Cet article érige en infraction pénale l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient considérées comme si elles étaient authentiques. Les Etats Parties peuvent remettre une déclaration[48] exigeant une intention frauduleuse ou une autre intention similaire.

En droit suisse, si l'auteur n'est pas habilité à accéder aux données, la disposition pénale concernant la détérioration des données[49] est applicable. Si l'auteur intervient dans un processus de traitement des données et s'il y a transfert d'actifs et dommage, l'art. 147 CP[50] est applicable. Par ailleurs, l'infraction de faux dans les titres[51] ou de tentative de faux dans les titres vaut également pour les fichiers et données électroniques. La disposition de la Convention est ainsi couverte par le droit en vigueur. Il sera néanmoins nécessaire d'émettre une déclaration selon laquelle un élément constitutif de l'infraction supplémentaire est requis, à savoir qu'il y a intention de produire un dommage ou un avantage.

45 Voir ch. 2.2.1.
46 Notamment en ce qui concerne la production et l'importation de données.
47 En particulier les art. 143 et 143bis CP.
48 Art. 40 de la Convention.
49 Art. 144bis , ch. 1, CP.
50 Utilisation frauduleuse d'un ordinateur.
51 Art. 251 en relation avec l'art. 110, al. 4, CP.

2.2.7 Art. 8 – Fraude informatique

L'art. 8 de la Convention érige en infraction le fait intentionnel et sans droit de causer un préjudice patrimonial à une autre personne dans l'intention frauduleuse ou délictueuse d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui. Le préjudice doit se faire par introduction, altération, effacement ou suppression de données informatiques (let. a) ou par une autre forme d'atteinte au fonctionnement d'un système informatique (let. b).

L'art. 147 CP punit l'utilisation frauduleuse d'un ordinateur. Contrairement à l'escroquerie « classique »[52], il couvre également le cas dans lequel l'auteur n'a pas induit la personne lésée en erreur en vue du transfert d'actifs, mais a simplement manipulé des données[53]. Il y a par exemple utilisation de données inexactes au sens de la disposition pénale lorsque l'auteur modifie, efface, déplace ou altère des données de manière contraire aux faits. Des données peuvent aussi être inexactes lorsqu'elles sont enregistrées au mauvais moment. Est également punissable quiconque influe, en recourant à « un procédé analogue », sur un processus de traitement ou de transmission de données et provoque ainsi un transfert d'actifs ou le dissimule.

L'art. 8 de la Convention est couvert par l'art. 147 CP. Dans les deux cas, le transfert d'actifs fait partie de l'élément objectif de l'infraction et doit donc être effectif pour que celle-ci soit accomplie. Il n'est pas nécessaire que l'auteur en tire réellement un profit. Si, en vue du transfert d'actifs, l'auteur a induit la personne lésée en erreur, c'est la norme sur l'escroquerie « classique » (art. 146 CP) qui s'applique, même si des processus de traitement de données sont en jeu; il prime alors l'art. 147[54].

2.2.8 Art. 9 – Infractions se rapportant à la pornographie enfantine

Selon l'art. 9 de la Convention, doit être punissable quiconque utilise un système informatique pour offrir, mettre à disposition, diffuser, transmettre, se procurer, posséder ou produire par le biais d'un système informatique du matériel de pornographie enfantine.

L'art. 197, ch. 3 et 3bis, CP punit ces actes, notamment la possession de pornographie enfantine sur supports de données électroniques ou le téléchargement de ce même matériel. Le droit suisse couvre également les « images réalistes » mentionnées à l'art. 9, par. 2, let. c, de la Convention[55]. Il n'est pas nécessaire d'utiliser la possibilité de faire une réserve à ce sujet.

L'art. 9, par. 2, let. b, de la Convention se réfère à la représentation d'une personne « qui apparaît comme un mineur ». Cette disposition n'est pas totalement limpide et le rapport explicatif n'en éclaire pas le sens. S'il s'agit de personnes dont on ne peut conclure qu'elles sont mineures, le juge suisse peut déterminer, dans le cadre de l'appréciation des preuves, dans quelle mesure il s'agit d'un acte commis avec un enfant entraînant une punissabilité de l'auteur. Les exigences de la Convention sont alors remplies. S'il s'agit cependant, comme semble l'indiquer la comparaison des

52 Sanctionnée par l'art. 146.
53 Cf. N. Schmid, *loc. cit.*, § 7 n. 1.
54 Cf. N. Schmid, *loc. cit.*, § 7 n. 161.
55 Cf. le message du 10 mai 2000 concernant la modification du CP et du CPM, FF **2000** 2807 s.

différentes versions linguistiques de la Convention, de la représentation d'un adulte qui se donne l'apparence d'un enfant, elle n'est pas punissable en droit suisse. Il est vrai que de telles représentations peuvent avoir un effet corrupteur sur leur spectateur, mais leur danger potentiel et leur gravité véritable ne sauraient être comparés aux conséquences fatales de la « vraie » pornographie enfantine pour ses acteurs et ses consommateurs. Il ne semble pas opportun d'étendre en ce sens la norme pénale. Nous proposons donc de déposer une réserve selon laquelle la let. b du par. 2 ne s'appliquera pas.

Selon la doctrine et la jurisprudence dominantes, les mineurs de moins de seize ans sont considérés comme « enfants » au sens de l'art. 197 CP[56]. La protection offerte par l'art. 187 CP[57] s'étend à la même catégorie d'âge. Plusieurs pensent toutefois que cette limite ne devrait pas être le seul critère de l'interdiction absolue de représentations pornographiques. Ils préconisent de punir également la représentation d'adolescents de plus de seize ans s'ils sont physiquement peu développés, et de tenir compte de l'impression produite et du fait que le matériel s'adresse manifestement à un spectateur pédophile.

Il est possible, dans le cadre de la mise en œuvre et de la ratification de la Convention, de déposer une déclaration[58] selon laquelle l'âge limite visé à l'art. 9, par. 3, de la Convention est de seize ans. Bien que la Suisse n'applique pas dans tous les cas un âge limite de seize ans, il convient qu'elle fasse usage de cette possibilité.

Il est vrai cependant que l'idée d'un âge limite fixé strictement à 18 ans a tendance à s'imposer sur le plan international. On examinera s'il est nécessaire et opportun d'adapter le droit suisse, en relation avec les actes sexuels commis avec des enfants et les représentations de tels actes, dans le contexte d'une éventuelle mise en œuvre de la Convention du Conseil de l'Europe du 25 octobre 2007 pour la protection des enfants contre l'exploitation et les abus sexuels.

2.2.9 Art. 10 - Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Selon la terminologie d'usage en Suisse, il est question dans cette disposition de droit d'auteur et de droits voisins[59]. La Suisse a ratifié toutes les conventions qui sont mentionnées à l'art. 10 de la Convention sur la cybercriminalité, soit:

- la Convention de Berne pour la protection des œuvres littéraires et artistiques, dans sa version révisée à Paris le 24 juillet 1971[60];
- la Convention internationale du 26 octobre 1961 sur la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion[61];

56 Cf. Schwaibold/Meng, Basler Kommentar, *op. cit.*, n. 21 ss *ad* art. 197.
57 Actes d'ordre sexuel avec des enfants.
58 Art. 40 de la Convention.
59 La terminologie utilisée dans la version française de l'art. 10 est particulière (ainsi « copyright » a été traduit par « propriété intellectuelle » au lieu de « droit d'auteur »), et ne reprend pas toujours les titres officiels en français des accords internationaux qui sont cités (voir ADPIC et WCT). A noter que l'expression « droits connexes » est utilisée au niveau international, mais que ces droits sont habituellement désignés en Suisse par « droits voisins » (*verwandte Schutzrechte*).
60 RS **0.231.15**.
61 Convention de Rome, RS **0.231.171**.

- l'Accord sur les aspects de propriété intellectuelle qui touchent au commerce[62];
- le Traité de l'OMPI du 20 décembre 1996 sur le droit d'auteur[63];
- le Traité de l'OMPI du 20 décembre 1996 sur les interprétations et exécutions et les phonogrammes[64].

La révision partielle de la loi du 9 octobre 1992 sur le droit d'auteur[65] qui est entrée en vigueur le 1er juillet 2008 adapte la législation suisse à ces deux derniers instruments de l'OMPI (WCT et WPPT). Le WCT et le WPPT ont été ratifiés et sont entrés en vigueur pour la Suisse en même temps que cette modification.

Comme le précise le rapport explicatif du Conseil de l'Europe, «l'emploi du membre de phrase «conformément aux obligations que celles-ci a souscrites» dans les deux paragraphes spécifie qu'une Partie contractante à la présente Convention n'est pas tenue d'appliquer les instruments mentionnés auxquels elle n'est pas partie»[66]. La Convention est donc formulée de telle manière que les Etats Parties n'encourent pas d'obligation en vertu des conventions internationales qu'ils n'ont pas encore ratifiées. La Suisse étant liée tant par la Convention de Berne, la Convention de Rome, l'Accord ADPIC, le WCT et le WPPT, c'est à la lumière de ces conventions qu'il faut examiner les obligations qu'elle doit remplir en vertu de la Convention sur la cybercriminalité.

La Suisse a reconnu dans sa LDA les droits prévus par les conventions qu'elle a ratifiées et dans les art. 67 à 69a de cette même loi elle a érigé en infractions pénales les violations correspondantes du droit d'auteur et des droits voisins. Ces dispositions permettent également de poursuivre - comme l'art. 10 de la Convention l'exige - les infractions qui seraient commises «au moyen d'un système informatique».

La LDA remplit également les exigences posées quant au fait que les actes punissables doivent avoir été commis «délibérément» puisqu'elle incrimine les infractions commises «intentionnellement». Elle respecte également la condition selon laquelle les violations doivent avoir lieu «à l'échelle commerciale» puisque les infractions «par métier» sont poursuivies d'office et va même au-delà puisqu'elle permet la poursuite sur plainte dans les autres cas.

Par ailleurs, la LDA a été révisée et adaptée au WCT et au WPPT, de sorte que la Suisse remplit toutes les obligations imposées par l'art. 10 de la Convention sur la cybercriminalité.

2.2.10 Art. 11 – Tentative et complicité

L'art. 11 de la Convention est couvert par le droit pénal suisse en vigueur, notamment par les art. 22, 24 et 25.

2.2.11 Art. 12 – Responsabilité des personnes morales

En vertu de cette disposition, les personnes morales doivent pouvoir être rendues responsables des infractions visées par la Convention lorsqu'elles sont commises pour leur compte par une personne physique qui exerce un pouvoir de direction en

62 ADPIC, Annexe 1.C à l'Accord du 15 avril 1994 instituant l'organisation mondiale du commerce; RS **0.632.20**.
63 WCT; RS **0.231.151**.
64 WPPT; RS **0.231.171.1**.
65 LDA; RS **231.1**.
66 Voir ch. 110 *in fine* du rapp. expl. (lien disponible sous note 1).

leur sein (par. 1). Par ailleurs, les Etats Parties doivent s'assurer qu'une entreprise puisse être tenue pour responsable lorsqu'une personne sous son autorité commet une infraction visée par la Convention pour son propre compte et que cette infraction est imputable à un défaut de supervision de la part d'une personne qui exerce un pouvoir de direction au sein de l'entreprise (par. 2).

La responsabilité peut être civile, administrative ou pénale (par. 3) et ne doit pas exclure une éventuelle responsabilité pénale de la personne physique qui a commis l'infraction (par. 4).

Parmi les traités récents de droit pénal international, nombreux sont ceux qui prévoient des règles, parfois identiques, concernant la responsabilité des entreprises. Par exemple, la Convention pénale sur la corruption du Conseil de l'Europe du 27 janvier 1999[67] prévoit la responsabilité des personnes morales, sans préciser son caractère civil, administratif ou pénal[68]. Ces traités ne déclarent délibérément pas illicite le principe - encore bien répandu malgré une tendance contraire sur le plan international - selon lequel les personnes morales ne peuvent pas assumer de responsabilité pénale. Cependant les Etats Parties doivent s'assurer que les personnes morales sont aussi soumises à des sanctions ou à des mesures appropriées, y compris des sanctions pécuniaires[69].

La responsabilité pénale de l'entreprise a été introduite dans le droit suisse le 1er octobre 2003[70]. Les nouvelles dispositions prévoient une responsabilité primaire de l'entreprise pour certaines catégories d'infractions lorsque l'on peut lui reprocher de n'avoir pas pris toutes les mesures d'organisation raisonnables et nécessaires pour empêcher l'infraction[71]. Cependant, les actes pénalisés par la Convention[72] n'en font pas partie[73].

La Suisse a en même temps instauré une responsabilité pénale subsidiaire générale de la personne morale dans le cas où une infraction ne peut être imputée à aucune personne physique déterminée en raison du manque d'organisation de l'entreprise[74]. La peine prévue est une amende pouvant aller jusqu'à cinq millions de francs. Cette responsabilité pénale s'étend à tous les crimes et délits sanctionnés par le droit suisse[75] ; elle recouvre donc les infractions visées par la Convention. Cette norme va plus loin que le texte de la Convention dans le sens où celui-ci se limite aux infractions commises pour le compte de l'entreprise par un membre de sa direction, tandis que le CP punit tous les crimes et délits commis dans l'exercice d'activités commerciales conformes aux buts de l'entreprise. Par contre, l'art. 102, al. 1, CP permet de sanctionner une personne morale uniquement lorsque l'acte délictueux ne peut être imputé à aucune personne physique.

L'art. 12, par. 4, de la Convention statue que la responsabilité pénale de la personne morale est établie sans préjudice de celle de la personne physique. On peut se

67 STE n° 173, art. 18 ; RS **0.311.55**.
68 Son rapport explicatif (ch. 86) mentionne cependant que les Etats Parties ne sont pas tenus d'introduire la responsabilité pénale des personnes morales.
69 Cf. art. 13 de la Convention.
70 Aujourd'hui, art. 102 et 102*a* CP
71 Art. 102, al. 2, CP.
72 Art. 2 à 9.
73 La liste comprend notamment les actes de corruption et le blanchiment d'argent.
74 Art. 102, al. 1, CP.
75 Infractions passibles d'une peine privative de liberté ou d'une peine pécuniaire ; cf. art. 10 CP.

demander s'il s'agit d'obliger les Etats Parties à prévoir une responsabilité pénale parallèle. Le rapport explicatif de la Convention ne donne pas d'indications à ce sujet.

La responsabilité subsidiaire des personnes morales en droit suisse n'exclut pas la punissabilité de la personne physique. Elle s'applique lorsque l'auteur ne peut pas être puni en raison du manque d'organisation de l'entreprise. L'art. 102, al. 1, CP n'est donc pas en contradiction avec l'art. 12, par. 4, de la Convention. Témoin le cas dans lequel il est possible de déterminer la personne physique impliquée et son comportement une fois l'entreprise condamnée : rien ne s'oppose alors, en principe, à ce que tant la personne physique que la personne morale soient punies[76].

Outre la responsabilité pénale de l'entreprise, la responsabilité de droit administratif permet de prendre des sanctions pour éviter des dommages futurs, par exemple en retirant une autorisation ou en refusant d'autoriser une entreprise à exercer ses activités dans un domaine particulier. Le droit suisse connaît plusieurs mécanismes de cet ordre, qui ne peuvent toutefois pas être appliqués indistinctement à toutes les entreprises et qui n'ont de portée que dans certains secteurs du marché et de l'économie. Ainsi, il est possible d'infliger des sanctions administratives aux entreprises soumises à la surveillance de l'Etat. L'Autorité fédérale de surveillance des marchés financiers peut par exemple retirer leur autorisation d'exercer aux établissements bancaires qui ne remplissent plus les conditions ou qui ont enfreint gravement leurs obligations légales[77].

Les sociétés et les établissements qui ont un but illicite ou contraire aux mœurs ne peuvent acquérir la personnalité. Elles doivent donc être dissoutes et leur fortune est dévolue à la corporation publique[78]. Enfin il existe des moyens et instruments civils pour engager la responsabilité d'entreprises pour le compte desquelles des infractions ont été commises par une personne qui exerce un pouvoir de direction en leur sein ou qui a négligé ses devoirs de surveillance concernant une infraction commise par un subordonné.

On peut donc considérer que le droit suisse répond aux exigences de l'art. 12 de la Convention. La norme suisse relative à la responsabilité pénale subsidiaire de l'entreprise va en partie plus loin que ne l'exige la Convention en garantissant que les crimes et délits commis dans le cadre du but de l'entreprise ne demeurent pas impunis lorsqu'ils ne peuvent être attribués à aucune personne physique. Cette responsabilité subsidiaire pourrait précisément être d'une grande importance dans le contexte des infractions visées par la Convention car il est vraisemblablement très difficile de déterminer quel est l'auteur physique d'une cyber-infraction. Il n'est donc pas utile d'inclure les infractions visées par la Convention dans la disposition du code pénal statuant une responsabilité primaire de l'entreprise, ni sous forme de liste ni de manière générale[79].

2.2.12 Art. 13 – Sanctions et mesures

Le par. 1 de cette disposition oblige les Etats Parties à prévoir des sanctions effectives, proportionnées et dissuasives, au nombre desquelles figure aussi la peine

76 Cf. Niggli/Gfeller, Basler Kommentar, Bâle 2007, n. 113 *ad* art. 102.
77 Art. 23^{quinquies} de la loi du 8 novembre 1934 sur les banques, RS **952.0**.
78 Art. 52 et 57 du code civil.
79 Au contraire de la Convention pénale sur la corruption dont il a été question plus haut, car les infractions visées par cette Convention ont un lien incomparablement plus étroit avec l'activité économique de l'entreprise.

privative de liberté, afin de réprimer les infractions établies en application de la Convention. Le droit suisse en vigueur répond à cette exigence en ce sens que les infractions correspondantes sont toutes des délits au moins.

Le par. 2 dit que les personnes morales tenues pour responsables en application de l'art. 12 doivent elles aussi faire l'objet de sanctions ou de mesures pénales ou non pénales répondant aux mêmes critères, celles-ci comprenant aussi des sanctions pécuniaires. Le droit suisse satisfait à ces exigences de la Convention en ce sens que les jugements et décisions rendus par des autorités civiles ou administratives peuvent prévoir des sanctions de nature pécuniaire à l'encontre d'entreprises fautives, parallèlement à la responsabilité pénale subsidiaire des entreprises[80], lesquelles encourent à ce titre des amendes allant jusqu'à cinq millions de francs. Ces sanctions sont effectives, proportionnées et dissuasives.

2.2.13 Art. 14 – Portée d'application des mesures du droit de procédure

Le par. 2, let. b, pose le principe selon lequel les dispositions du droit de procédure prévues aux art. 14 à 21 s'appliquent non seulement à la poursuite d'infractions au sens de la Convention, mais aussi, et de manière générale, à toutes les infractions commises au moyen d'un système informatique. Le par. 2, let. c, précise que ces dispositions s'appliquent à la collecte des preuves électroniques de toute infraction pénale. Par cette disposition, la Convention entend garantir que les données électroniques enregistrées dans le cadre de procédures pénales puissent également être utilisées comme moyen de preuve, au même titre que des preuves non électroniques[81].

C'est en considération de ce champ d'application étendu qu'il convient d'examiner dans quelle mesure le droit de procédure nécessite d'être adapté et si notamment les règles concernant la surveillance, le séquestre, la confiscation et, de manière générale, l'administration des preuves s'appliquent aux médias électroniques.

Sur le plan national, le droit de procédure au sens large repose d'une part sur les codes de procédure pénale de la Confédération et des cantons et d'autre part sur la loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[82] et son ordonnance d'exécution[83], entrées en vigueur le 1er janvier 2002. La LSCPT continuera de s'appliquer après l'entrée en vigueur du code de procédure pénale du 5 octobre 2007[84] (exécution de la surveillance), mais les règles de procédure pénale qu'elle contient[85] seront intégrées dans ce code. Nous nous réfèrerons ici au droit actuel, sauf lorsque le CPP prévoit de nouvelles normes importantes.

L'art. 14, par. 3, let. b, de la Convention porte sur les « groupes d'utilisateurs fermés », par exemple les réseaux informatiques internes d'une entreprise. Selon les art. 1, al. 4, et 15, al. 8, LSCPT, les exploitants de réseaux de télécommunication internes et de centraux domestiques sont tenus de tolérer une surveillance et de

80 Cf. commentaire de l'art. 12.
81 Ch. 141 du rapp. expl.
82 LSCPT, RS **780.1**.
83 OSCPT, RS **780.11**.
84 CPP, FF **2007** 6583, entrée en vigueur prévue le 1.1.2011.
85 Art. 3 à 10 LSCPT.

fournir les renseignements nécessaires. Il est donc en principe possible de se procurer et de sauvegarder les données dans ce cadre, même dans le domaine non public[86].

2.2.14 Art. 15 – Conditions et sauvegardes

L'art. 15 prévoit l'obligation pour les Etats Parties de respecter les droits de l'homme et les libertés fondamentales et de les garantir dans ce contexte. En particulier, le principe de la proportionnalité des actes de procédure doit être respecté ; le type de mesures de contrainte doit correspondre à la gravité et au genre de l'infraction faisant l'objet de l'instruction et ne pas être disproportionné en termes de conséquences ni de temps requis.

2.2.15 Art. 16 – Conservation rapide de données informatiques stockées

L'art. 16 de la Convention oblige les Etats Parties à faire en sorte que les autorités d'instruction compétentes puissent ordonner ou obtenir la conservation rapide de données informatiques stockées[87]. Lorsque les autorités ordonnent à une personne, par exemple un fournisseur de service, de conserver des données, cette personne est tenue de les préserver contre toute modification pendant une période déterminée.

Les codes de procédure pénale en vigueur en Suisse permettent de conserver rapidement les données électroniques, en respectant le principe de la proportionnalité, dans le cadre de la collecte et de la conservation des moyens de preuve ordonnées par les autorités d'instruction. Le code de procédure pénale du 5 octobre 2007[88] considère les données et supports de données électroniques comme des moyens de preuve matériels, qui peuvent être versés au dossier[89] ou soumis à une perquisition[90].

La Convention suggère qu'une conservation immédiate peut aussi être obtenue en obligeant des tiers (dignes de confiance) à conserver des données (*« injonctions de conservation »*). Toutefois, elle n'oblige pas les Etats Parties à prévoir une telle solution[91]. Pour répondre à ses exigences, il suffit que l'autorité compétente assure elle-même la conservation des données, après saisie des moyens de preuve.

Le droit suisse en vigueur satisfait de manière générale à cette exigence, du moins partiellement, c'est-à-dire en ce qui concerne certaines données en possession des fournisseurs de services Internet. La LSCPT exige de ces derniers qu'ils conservent les données relatives au trafic et à la facturation pendant une période de six mois[92]. Les fournisseurs peuvent aussi être enjoints, par une décision de l'autorité compétente, de conserver provisoirement des données. Conférer à l'autorité la compétence d'ordonner à toute personne de conserver des données irait toutefois

86 Sous réserve naturellement de la disponibilité des données.
87 Y compris les données de transmission, c'est-à-dire les données relatives au moyen, à la durée et à l'heure de la communication ainsi qu'aux personnes impliquées. Cf. art. 2, let. g, OSCPT.
88 Cf. commentaire de l'art. 14 de la Convention.
89 Art. 192 ss CPP.
90 Art. 246 ss CPP.
91 Voir ch. 160 du rapp. expl.
92 Art. 15, al. 3, LSCPT : données d'identification et données relatives au trafic et à la facturation. Le délai de conservation obligatoire sera probablement étendu à un an (bien que la Convention ne l'exige pas ; voir ch. 161 *in fine* du rapp. expl.).

trop loin dans ce contexte et ne serait guère compatible avec l'art. 15 de la Convention (principe de proportionnalité). Le droit suisse actuel répond donc de manière satisfaisante aux exigences de cette disposition de la Convention.

2.2.16 Art. 17 – Conservation et divulgation rapides de données relatives au trafic

L'art. 17 de la Convention exige que les données relatives au trafic[93] au sens de l'art. 16 puissent également être conservées dans le cas où plusieurs fournisseurs de services ont participé à la transmission de la communication (par. 1, let. a).

Le droit suisse satisfait aux exigences du par. 1, let. a. Selon l'art. 15, al. 3, LSCPT, les fournisseurs sont tenus de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation. Si plusieurs fournisseurs participent à la communication, l'autorité donne à l'un d'eux un mandat officiel de surveillance, si bien que tous les autres sont tenus de lui transmettre les données en leur possession (art. 15, al. 2, LSCPT). Le fait que plusieurs fournisseurs de services aient participé à une communication n'empêche donc en rien la conservation rapide de données relatives au trafic.

L'art. 17, par. 1, let. b, de la Convention prévoit que le fournisseur de services que l'on oblige à conserver les données relatives au trafic les divulgue aux autorités compétentes de manière à leur permettre d'identifier les autres fournisseurs et la voie par laquelle la communication a été transmise. L'autorité qui en fait la demande doit spécifier de manière suffisamment précise quelles données doivent lui être transmises. Il n'est pas encore question, à ce stade, d'identifier nommément l'auteur ou le destinataire d'une information[94].

Après l'entrée en vigueur du CPP[95], le ministère public pourra exiger, pour tous les crimes et délits, que lui soient fournies les données permettant l'identification des usagers (auteur, destinataire et moment de la transmission) ainsi que les données relatives au trafic et à la facturation (art. 273 CPP). L'ordre de surveillance devra être soumis à l'autorisation du tribunal des mesures de contrainte, mais indépendamment d'une liste d'infractions et avec la possibilité de demander des données avec effet rétroactif. Le fait que cette disposition ne s'applique pas aux simples contraventions n'est pas incompatible avec la Convention, en vertu du principe de proportionnalité[96]. Le droit suisse actuel satisfait donc aux exigences de la Convention.

Par ailleurs, l'art. 14, al. 4, LSCPT restera applicable à toutes les infractions commises au moyen d'Internet[97]. Il contraint le fournisseur à donner à l'autorité compétente toutes les indications dont il dispose permettant d'identifier l'auteur. En font partie les données qui permettent de déterminer le « chemin de communication ». L'art. 14, al. 4, LSCPT s'applique à l'ensemble du domaine

93 Les données relatives au trafic – données concernant l'origine, la destination, la durée ou l'itinéraire de la communication – ne comprennent pas forcément l'adresse ou l'identité de l'expéditeur (art. 1, let. d, de la Convention, cf. ch. 30 du rapp. expl., lien disponible sous note 1). Il peut s'agir d'une adresse IP. Les Etats Parties sont libres de protéger les catégories de données de leur choix (ch. 31 du rapp. expl.).

94 Voir ch. 169 du rapp. expl.

95 Prévue pour le 1.1.2011.

96 Art. 15 de la Convention.

97 Ce terme peut être considéré comme restrictif par rapport aux infractions commises « au moyen d'un système informatique ».

Internet[98] et se réfère tant aux adresses IP statiques que dynamiques[99]. Dans les deux cas, il ne s'agit pas d'une mesure de surveillance au sens ordinaire de la LSCPT ; l'autorité d'instruction peut directement présenter une demande au service compétent, indépendamment du type d'infraction invoqué[100].

2.2.17 Art. 18 – Injonction de produire

Selon l'art. 18, par. 1, let. a, de la Convention, l'autorité d'instruction doit pouvoir obliger toute personne à communiquer les données informatiques enregistrées dont elle dispose. Cette disposition a son équivalent en droit suisse (obligation de produire des pièces appliquée aux personnes non accusées) et se retrouvera aussi dans le CPP[101]. En cas de refus, il est possible d'ordonner des mesures de contrainte.

En outre, les fournisseurs de service (par. 1, let. b) doivent être tenus de communiquer, sur injonction de l'autorité compétente, les données relatives aux abonnés[102], mais non les données relatives au trafic ou aux contenus. Cette disposition de la Convention ne règle donc pas l'identification des participants à une transmission de données concrète. Elle porte sur l'identification de participants possibles au réseau. La question de leur surveillance ne se pose pas[103]. Comme on l'a exposé à propos de l'art. 17 de la Convention, l'autorité d'instruction peut demander des informations sur les données permettant l'identification des usagers et sur les données de trafic et de facturation pour tous les crimes et délits[104]. L'ordre de surveillance devra être soumis à l'autorisation du tribunal des mesures de contrainte, mais indépendamment d'une liste d'infractions et avec la possibilité de demander des données avec effet rétroactif.

L'art. 14, al. 4, LSCPT s'applique ici également[105]. Le fournisseur doit en particulier livrer le nom et l'adresse du participant et d'autres paramètres de communication au sens de la loi du 30 avril 1997 sur les télécommunications[106].

L'art. 18, par. 1, let. b, de la Convention se limite à des données dont dispose le fournisseur et ne prescrit pas à ce dernier quelles informations doivent être conservées (donc aptes à être produites), ni combien de temps. Si, en l'espèce, les données ne sont pas (ou plus) disponibles sur la base de la réglementation nationale, cela ne crée pas une divergence avec la Convention.

Le droit suisse répond donc aux exigences de l'art. 18 de la Convention, notamment si l'on tient compte des dispositions du CPP.

98 Cf. décision de la commission de recours du DETEC du 27.4.2004, J-2003-162; consultable à l'adresse http://www.reko-inum.admin.ch.

99 Une adresse IP *statique* (protocole Internet) est formée d'une série unique de quatre nombres attribuée à un ordinateur relié à Internet. L'adresse IP *dynamique* n'est pas durablement attribuée à un raccordement fixe. Elle est mise à la disposition de l'utilisateur par le fournisseur de services pour la durée de la session Internet. Chaque jour, un grand nombre d'utilisateurs utilisent la même adresse. Techniquement, il faut chercher dans le fichier journal pour retrouver l'utilisateur de l'adresse à un moment donné dans le passé.

100 La liste d'infractions de l'art. 3 LSCPT n'est pas applicable.

101 Cf. art. 263 ss CPP, notamment art. 265 (Obligation de dépôt).

102 Par ex. identité de l'abonné, informations sur les paiements.

103 La liste d'infractions de l'art. 3 LSCPT n'est pas applicable.

104 Art. 273 CPP.

105 Cf. plus haut.

106 LTC, RS **784.10**.

2.2.18 Art. 19 – Perquisition et saisie de données informatiques stockées

L'art. 19, par. 1 et 3, de la Convention engage les Etats Parties à prévoir des règlementations habilitant les autorités compétentes à perquisitionner et à saisir des données informatiques enregistrées et des supports de données sur leur territoire. L'objectif est de garantir que les données informatiques puissent être saisies comme les biens meubles et que les autorités puissent y accéder à cette fin. La saisie de l'ordinateur lui-même doit également être possible[107]. Les conditions de la perquisition doivent être les mêmes que lors d'une recherche classique de moyens de preuve.

Il ne s'agit pas ici de questions de droit des télécommunications ou de surveillance des télécommunications, mais d'une matière régie par les règles nationales concernant l'acquisition et la conservation des preuves. Ces dernières années, de nombreux cas[108] ont montré que les codes de procédure pénale cantonaux répondaient de manière suffisante à ces exigences et qu'il était possible en pratique de perquisitionner et de saisir des données et des ordinateurs. Le CPP prévoit lui aussi, en partie explicitement, la perquisition et le séquestre de données et supports informatiques[109].

L'art. 19 se réfère aux données informatiques enregistrées et peut être appliqué en principe contre n'importe qui. Reste à savoir dans quelle mesure ces possibilités d'accès offertes aux autorités de poursuite pénale s'étendent aux données stockées chez les fournisseurs de service (par ex. les contenus appartenant aux abonnés) et s'il s'ensuit une restriction du secret des télécommunications. Le texte de la Convention ne livre aucun indice à ce sujet. Cependant, le rapport explicatif expose que les Etats demeurent libres, dans ce domaine, de protéger les communications en tant que telles. Par exemple, une information envoyée par mail, enregistrée provisoirement chez le fournisseur et qui n'a pas encore été appelée par le destinataire peut être considérée comme une partie de la communication[110], ce qui lui confère une protection particulière : elle ne peut être divulguée par le fournisseur de services que sur décision de l'autorité, les conditions requises étant réunies. Les données ne sont plus protégées par le secret des télécommunications au moment où elles sont stockées sur un support matériel appartenant au destinataire. Elles peuvent alors être séquestrées[111]. L'art. 19 de la Convention ne peut donc pas être utilisé pour saper ou éluder le secret des télécommunications.

Le par. 2 prévoit la possibilité que les autorités, ayant accédé à un premier système informatique, accèdent à un deuxième système pour le perquisitionner, dans les limites du droit. L'extension de la perquisition, par exemple à un système informatique relié au premier, peut donc être prévue par le droit national. La disposition interdit expressément la perquisition de supports de données sur le territoire d'un autre Etat à moins que certaines conditions bien particulières ne soient réunies (art. 32 de la Convention) ou que l'entraide judiciaire n'ait été accordée. Il

107 Voir ch. 187 du rapp. expl. (lien disponible sous note 1).
108 Notamment lors d'enquêtes de la police et du juge d'instruction dans le domaine de la pornographie enfantine.
109 Art. 246 ss et 263 ss CPP.
110 Voir ch. 190 du rapp. expl.
111 Le cas est comparable à un courrier postal qui est protégé par le secret postal. Un jour plus tard, intégrée par exemple à la comptabilité du destinataire, la lettre peut être séquestrée au cours d'une perquisition puis appréciée.

est aujourd'hui possible, dans certains cas et en vertu du droit national, d'accéder à un système relié à un autre système informatique dans le cadre de la perquisition[112]. Il faut cependant que l'autorisation de perquisitionner lui soit étendue. La formulation de la disposition de la Convention[113] tient compte de ce fait.

L'art. 19, par. 4, de la Convention prévoit une obligation pour les tiers (par ex. un administrateur de système) d'informer les autorités afin que celles-ci puissent accéder aux données. La LSCPT prévoit une obligation de ce type dans certains domaines[114]. Le devoir de coopération mentionné par la Convention reste raisonnable et proportionné. Ainsi, la divulgation d'un mot de passe à la demande de l'autorité peut être raisonnable dans certains cas mais non dans d'autres[115].

Ces obligations vont-elles au-delà de l'obligation de témoigner usuelle en procédure pénale ou de l'obligation des tiers de produire des pièces[116] ? Vu que la Convention limite l'obligation de fournir des informations à des cas raisonnablement nécessaires, après injonction de l'autorité, la possibilité qu'offre le droit suisse aux autorités d'instruction d'ordonner la production de pièces satisfait sans doute aux exigences de ce texte. Il ressort en particulier du rapport explicatif[117] que la norme vise les administrateurs de systèmes ou les personnes disposant d'une fonction de surveillance similaire sur un système informatique. Dans ces cas-là, le droit suisse permet d'examiner dans le cas d'espèce dans quelle mesure la personne concernée a une position de garant, ce qui permet de sanctionner la contravention contre une ordonnance de production de pièces en vertu de l'art. 305 CP[118].

2.2.19 Art. 20 – Collecte en temps réel de données informatiques

L'art. 20 de la Convention régit la collecte en temps réel de données relatives au trafic par les autorités compétentes. Les Etats Parties doivent habiliter celles-ci à obliger les fournisseurs de services à collecter ou enregistrer ces données. La Convention autorise les Etats à dresser une liste d'infractions comme condition de ces mesures et à émettre une réserve à ce sujet[119].

Le droit suisse permet de collecter en temps réel les données permettant l'identification des usagers (de même que les données relatives aux contenus). Ce type de surveillance ne peut toutefois être exercé que dans le cadre des infractions listées dans la LSCPT[120]. Cette liste est reprise dans le CPP pour ce qui est des données relatives aux contenus. Quant aux données relatives au trafic et à la facturation ainsi qu'aux données permettant l'identification des usagers, le CPP va plus loin que la LSCPT puisqu'il permet aux autorités de les demander en cas de crime ou de délit[121]. Puisqu'il est possible d'émettre une réserve conformément à l'art. 14, par. 3, de la Convention, aucune adaptation du droit suisse n'est nécessaire.

112 Concernant certains réseaux, l'autorité d'instruction n'est pas forcément consciente du fait que les systèmes sont reliés.
113 « Légalement accessible ».
114 Art. 14, al. 4 et art. 15, al. 8, LSCPT (obligation des propriétaires de réseaux de télécommunication internes et de centraux domestiques d'en garantir l'accès).
115 Voir ch. 202 du rapp. expl. (lien disponible sous note 1) et art. 15 de la Convention.
116 L'obligation de produire des pièces n'implique pas pour les tiers qu'ils doivent coopérer à la recherche de preuves ; voir art. 265 CPP.
117 Ch. 200 ss du rapp. expl. (lien disponible sous note 1).
118 Entrave à l'action pénale ; cf. ATF 120 IV 106.
119 Art. 14, par. 3, en relation avec l'art. 42 de la Convention.
120 Art. 3 LSCPT.
121 Indépendamment de la liste des infractions ; art. 273 CPP.

2.2.20 Art. 21 – Interception de données relatives au contenu

L'art. 21 de la Convention règle la collecte en temps réel de données relatives au contenu par les autorités compétentes. Celles-ci ne peuvent y recourir ou y obliger un fournisseur qu'en relation avec un éventail d'infractions graves, déterminées par chaque Etat Partie, par exemple sous forme de liste. En Suisse, il est possible d'ordonner la surveillance en temps réel et l'enregistrement de données relatives au contenu d'une communication, en relation avec une des infractions de la liste de l'art. 3 LSCPT. Il n'y a donc pas lieu d'adapter la législation.

2.2.21 Art. 22 - Compétence

La Convention distingue entre compétence obligatoire et facultative des Etats Parties à l'égard des infractions pénales décrites dans la Convention, selon que l'infraction est commise sur leur territoire (principe de la territorialité, let. a du par. 1, disposition impérative) ou qu'elle est commise à bord d'un navire battant pavillon de l'Etat concerné (principe du pavillon, par. 1, let. b) ou d'un aéronef immatriculé selon les lois de cet Etat (par. 1, let. c). Les tribunaux suisses sont compétents selon l'art. 3 CP, l'art. 4, al. 2, de la loi fédérale du 23 septembre 1953 sur la navigation maritime sous pavillon suisse[122] et l'art. 97, al. 1, de la loi fédérale du 21 décembre 1948 sur l'aviation[123].

Selon la let. d du par. 1, chaque Etat Partie doit se déclarer compétent lorsque l'infraction est commise par un de ses ressortissants, si elle est punissable pénalement là où elle a été commise ou qu'elle ne relève de la compétence territoriale d'aucun Etat. La compétence des tribunaux suisses dans ce cas est établie par l'art. 7, al. 1, let. a, CP (principe de la personnalité active). Il n'y a donc pas lieu de déposer une réserve à ce sujet comme le permet l'art. 22, par. 2 (qui se réfère aux let. b à d).

Selon le par. 3 de cette disposition, les Etats Parties doivent établir leur compétence à l'égard de toute infraction visée par la Convention[124] lorsque l'auteur présumé est présent sur leur territoire et ne peut être extradé vers un autre Etat Partie au seul titre de sa nationalité. La Suisse connaît cette obligation d'ouvrir une poursuite pénale en cas de non-extradition (*aut dedere aut judicare*), statuée à l'art. 6 CP. L'art. 7 de la loi sur l'entraide pénale internationale[125] dispose qu'aucun citoyen suisse ne peut être extradé sans son consentement à un Etat étranger pour y faire l'objet d'une poursuite pénale. La Convention européenne d'extradition du 13 décembre 1957[126] règle l'extradition par les Etats de leurs propres ressortissants en son art. 6, qui prévoit la même obligation que la Convention sur la cybercriminalité. Les règles applicables à la poursuite pénale par délégation menée par la Suisse sont fixées aux art. 85 ss EIMP. Notons cependant que l'efficacité de ce type de poursuite dépend essentiellement des pièces de dossier et des moyens de preuve livrés par l'autre Etat.

122 RS **747.30**.
123 RS **748.0**.
124 L'infraction doit cependant être passible d'une peine privative de liberté d'au moins un an. Voir art. 24, par. 1, de la Convention.
125 EIMP ; RS **351.1**.
126 RS **0.353.1**.

2.3 Chapitre III: Coopération internationale

2.3.1 Considérations générales

Le système de coopération judiciaire internationale en matière pénale prévu dans la Convention sur la cybercriminalité a pour but de mettre en place un régime rapide et efficace de coopération. Ce régime prévoit que, sauf disposition contraire expressément prévue, les traités internationaux entre les Etats Parties ainsi que leur législation nationale s'appliquent. La Convention prévoit cependant des règles spécifiques pour certaines mesures qui dérogent à l'éventuelle réglementation applicable[127], notamment vu la rapidité requise pour les interventions peu compatibles avec la durée des procédures. Sa mise en œuvre nécessitera, vu la réglementation actuelle de la coopération judiciaire internationale en matière pénale, une modification de l'EIMP explicitée ci-dessous (voir ch. 2.3.9.1).

2.3.2 Art. 23 - Principes généraux relatifs à la coopération internationale

L'art. 23 énonce que les Etats Parties doivent coopérer les uns avec les autres « dans la mesure la plus large possible ». Ceci requiert de réduire autant que possible, au plan international, les obstacles à la circulation rapide et sans problème de l'information et des preuves. Cette clause, courante dans les instruments de lutte contre la criminalité, présente la particularité, en matière de cybercriminalité, de tendre à un échange plus rapide des informations que ce qui se produit dans les procédures habituelles de coopération judiciaire internationale pénale[128]. La portée générale de l'obligation de coopérer énoncée à l'art. 23 s'étend : a) à toutes les infractions pénales liées à des systèmes et données informatiques[129] ; b) à la collecte de preuves sous forme électronique se rapportant à une infraction pénale[130]. Les clauses du chapitre III sont ainsi applicables soit aux situations où l'infraction est commise à l'aide d'un système informatique, soit à celles où une infraction ordinaire, non commise à l'aide d'un système informatique, donne lieu à la collecte de preuves sous forme électronique[131].

2.3.3 Art. 24 - Extradition

L'art. 24, clause usuelle, fixe que l'obligation d'extrader s'applique uniquement[132] aux infractions définies aux art. 2 à 11 de la Convention. L'obligation d'extrader selon l'art. 24 est soumise aux conditions – cumulatives - que soient réalisées : a) la double incrimination[133] ; b) la peine privative de liberté pour une période maximale d'au moins un an d'emprisonnement, issues de l'art. 2, par. 1, de la Convention européenne d'extradition. Concernant la peine requise pour pouvoir procéder à

127 Ainsi en va-t-il, en rapport avec la réglementation suisse, de la divulgation rapide de données stockées, régie par l'art. 30 de la Convention, lesquelles données doivent être transmises à l'autorité requérante *avant* la clôture de la procédure, ainsi que de l'entraide dans la collecte en temps réel de données relatives au trafic réglementée à l'art. 33.

128 Voir ch. 16, 20 et 242 du rapp. expl. (lien disponible sous note 1).

129 C'est-à-dire les infractions visées par l'art. 14, par. 2, let. a et b de la Convention.

130 Art. 14, par. 2, let. c.

131 Voir ch. 243 du rapp. expl. (lien disponible sous note 1).

132 Il convient ici de relever la différence avec la coopération dans le domaine de l'entraide judiciaire qui, selon l'art. 23, a un champ d'application bien plus large : l'obligation de coopérer s'applique à la fois aux infractions pénales liées à des systèmes et des données informatiques ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale.

133 Législation concernée des deux Etats Parties.

l'extradition, il est renvoyé aux développements relatifs aux art. 2 à 11. En Suisse, la loi correspond à la Convention, car l'art. 35 EIMP prévoit que l'extradition peut être accordée s'il ressort des pièces jointes à la demande que l'infraction est frappée d'une sanction privative de liberté d'un maximum d'au moins un an ou d'une sanction plus sévère, aux termes du droit suisse et du droit de l'Etat requérant. En relation avec l'art. 24, par. 1 à 4, la Suisse ne subordonne pas l'extradition à l'existence d'un traité[134].

Selon l'art. 24, par. 5, l'extradition est soumise aux conditions prévues par le droit interne. La Suisse les règle aux art. 32 ss EIMP. Ainsi notre pays, en qualité d'Etat Partie requis, n'est pas tenu d'extrader s'il estime que les conditions prévues par le traité ou le droit interne applicables[135] ne sont pas réalisées, car la coopération est mise en œuvre selon les instruments en vigueur entre les Parties, dont la Convention européenne d'extradition du 13 décembre 1957 (CEExtr.) et ses deux Protocoles additionnels[136].

L'art. 24, par. 6 applique le principe *aut dedere, aut judicare*, soit extrader ou poursuivre. Les citoyens suisses ne peuvent être extradés qu'avec leur consentement écrit[137]. En cas de refus de la personne concernée et à la demande de la Partie requérante, la Suisse poursuivra[138] ladite personne en application de l'art. 24, par. 6, de la Convention et de l'art. 7, al. 1, CP. La Suisse renseignera la Partie requérante de l'issue de l'affaire. Par contre, si la Partie dont la demande d'extradition a été rejetée ne demande pas que l'affaire soit soumise aux autorités compétentes aux fins d'enquête et de poursuites, la Suisse ne sera pas tenue d'intervenir[139].

L'art. 24, par. 7, nécessite une communication de la Suisse au Secrétaire général du Conseil de l'Europe, selon laquelle l'Office fédéral de la justice (OFJ) est l'autorité suisse responsable des demandes d'extradition et d'arrestation provisoire[140]. L'application de cette disposition est limitée aux cas où aucun traité[141] n'a été conclu entre les Parties concernées. La désignation d'une autorité n'exclut cependant pas la possibilité de recourir à la voie diplomatique[142].

134 Art. 1, al. 1, let. a EIMP.

135 L'art. 37 EIMP prévoit notamment que l'extradition est refusée si la demande se fonde sur une sanction prononcée par défaut et que la procédure de jugement n'a pas satisfait aux droits minimums de la défense reconnus à toute personne accusée d'une infraction, à moins que l'Etat requérant ne donne des assurances jugées suffisantes pour garantir à la personne poursuivie le droit à une nouvelle procédure de jugement qui sauvegarde les droits de la défense. Cette disposition ajoute que l'extradition est également refusée si l'Etat requérant ne donne pas la garantie que la personne poursuivie ne sera pas condamnée à mort ou, si une telle condamnation a été prononcée, qu'elle ne sera pas exécutée, ou que la personne poursuivie ne sera pas soumise à un traitement portant atteinte à son intégrité corporelle.

136 RS **0.353.1**, **0.353.11** et **0.353.12**.

137 Art. 7 EIMP.

138 L'enquête et les poursuites doivent être menées avec célérité et avec le même sérieux que pour toute autre infraction de nature comparable qui serait instruite.

139 Si aucune demande d'extradition n'a été présentée ou que l'extradition a été refusée pour une raison autre que la nationalité, la Suisse n'aura aucune obligation de saisir ses autorités aux fins de poursuites. Voir ch. 251 du rapp. expl. (lien disponible sous note 1).

140 Art. 17, al. 2, EIMP.

141 En effet, si un traité d'extradition bilatéral ou multilatéral, telle la CEExtr. précitée, est en vigueur entre les Parties, celles-ci savent à qui adresser les demandes d'extradition ou d'arrestation provisoire sans qu'il soit besoin de tenir le registre des autorités concernées.

142 Voir ch. 252 du rapp. expl.

2.3.4 Art. 25 - Principes généraux relatifs à l'entraide

L'art. 25 oblige les Etats Parties (comme il ressort aussi de l'art. 23) à coopérer pour une très vaste catégorie d'infractions[143]. Selon l'art. 25, par. 2, de la Convention, la Suisse doit mettre en place les fondements juridiques lui permettant d'accorder les formes spécifiques de coopération décrites, en particulier celles figurant dans les art. 27 et 29 à 35 de la Convention. Ces mécanismes sont indispensables à une coopération efficace dans les affaires pénales en relation avec l'ordinateur[144]. Le détail de ces adaptations législatives est présenté au ch. 2.3.9.1.

L'art. 25, par. 3, de la Convention institue un moyen rapide d'entraide. Les données informatiques sont très volatiles. Il suffit de presser sur quelques touches ou d'utiliser un programme automatique pour les effacer, ce qui rend impossible de remonter jusqu'à l'auteur d'une infraction ou détruit les preuves de sa culpabilité. Certains types de données ne sont stockées que pour de courtes périodes avant d'être détruites. Dans des situations aussi urgentes, la demande comme la réponse doivent être rapides. L'art. 25, par. 3, institue donc l'entraide accélérée pour éviter que des informations ou des preuves essentielles ne soient perdues parce qu'elles auraient été effacées avant qu'une demande d'entraide n'ait pu être préparée et transmise et qu'une réponse n'ait pu être reçue. La Convention atteint ce résultat d'une part en autorisant les Etats Parties à présenter, en cas d'urgence, une demande de coopération par des moyens rapides de communication[145], et d'autre part en imposant à la Partie requise de répondre à une telle demande par des moyens rapides de communication. Chaque Etat Partie doit se donner les moyens d'appliquer cette mesure[146]. Les Etats Parties peuvent convenir de garanties de sécurité spéciales, dont le cryptage dans des affaires délicates[147]. La Partie requise peut exiger une confirmation officielle ultérieure, transmise par les voies classiques, ce qui correspond à la pratique suisse.

L'art. 25, par. 4, de la Convention énonce le principe général selon lequel l'entraide est soumise aux conditions fixées par les traités d'entraide et les dispositions du droit interne[148]. Cette clause usuelle vaut particulièrement concernant les mesures intrusives telles une opération de perquisition et de saisie qui sera exécutée uniquement si la Partie requise a la certitude que les conditions nécessaires à son prononcé sont réalisées[149]. Cette réglementation ne s'applique cependant pas en cas de « disposition contraire expressément prévue dans le présent chapitre ». La

143 Les art. 33 et 34 autorisent la modification du champ d'application de ces mesures ; il est donc renvoyé aux explications desdites dispositions.
144 Voir ch. 254 du rapp. expl.
145 Et non par les moyens classiques bien plus lents de transmission de documents écrits sous pli cacheté par la valise diplomatique ou par la poste.
146 La télécopie et le courrier électronique sont mentionnés à titre indicatif. Tout autre moyen rapide de communication, adapté aux circonstances d'espèce, peut être utilisé. Les progrès technologiques pourront offrir d'autres moyens rapides pour présenter une demande d'entraide.
147 Voir ch. 256 du rapp. expl. (lien disponible sous note 1).
148 Ceci afin de garantir les droits des personnes se trouvant sur le territoire de la Partie requise pouvant faire l'objet d'une demande d'entraide.
149 Voir ch. 257 du rapp. expl.

Convention contient plusieurs dérogations au principe général[150], notamment concernant les motifs de refus de l'entraide[151]. La coopération ne peut être refusée, selon l'art. 25, par. 4, pour les infractions des art. 2 à 11 de la Convention, au seul motif que l'infraction est considérée de nature fiscale, ce qui ne paraît pas problématique, car ces infractions ne constituent pas, en soi, des infractions fiscales, même si de telles méthodes peuvent être utilisées pour perpétrer des infractions fiscales. Il ne peut être exclu que certains Etats tentent d'utiliser les moyens rapides institués par la Convention sur la cybercriminalité pour obtenir, par exemple sous couvert d'une infraction ou de la recherche de moyens de preuves « informatiques », des informations que la Suisse ne veut pas communiquer.

L'art. 25, par. 5, fixe une clause habituelle relative à la double incrimination[152].

2.3.5 Art. 26 - Information spontanée

L'art. 26 étend à l'entraide une disposition dont l'origine se trouve à l'art. 10 de la Convention du 8 novembre 1990 relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime[153] et à l'art. 28 de la Convention pénale du 27 janvier 1999 sur la corruption[154]. Une réglementation en la matière se trouve également dans la plupart des traités actuels bilatéraux d'entraide judiciaire en matière pénale ainsi que dans l'art. 11 du Deuxième Protocole additionnel du 8 novembre 2001 à la Convention européenne d'entraide judiciaire en matière pénale[155], lequel, comme l'art. 26 de la Convention, contient aussi une clause de confidentialité. L'art. 26, disposition potestative, crée la possibilité pour les Parties, sans demande préalable, et éventuellement, selon son par. 2, sous condition[156], de se communiquer des informations sur des investigations ou des procédures dans leur objectif commun de lutte contre la criminalité[157]. L'échange d'informations

150 Voir ch. 258 du rapp. expl. : la première de ces dérogations découle de l'art. 25, par. 2, de la Convention, en vertu duquel chaque Partie est tenue d'accorder les formes de coopération énoncées dans les autres articles du chapitre (telles que la conservation, la collecte en temps réel de données, la perquisition et la saisie et la gestion d'un réseau 24/7), indépendamment de la question de savoir si ces mesures sont déjà inscrites dans ses instruments internationaux d'entraide ou sa législation en matière d'entraide. Une autre dérogation se trouve à l'art. 27 qui est toujours applicable à l'exécution de requêtes à la place d'une disposition du droit interne de la Partie requise régissant la coopération internationale en l'absence d'un traité d'entraide ou arrangement équivalent entre la Partie requérante et la Partie requise (système de conditions et de motifs de refus).

151 Voir également les explications présentées pour l'art. 27, par. 4.

152 Voir ch. 259 du rapp. expl. (lien disponible sous note 1) : en effet, vu les différences entre les ordres juridiques nationaux, des différences de terminologie et de classement des comportements criminels peuvent être constatés. Si le comportement constitue une infraction pénale dans les deux ordres juridiques, ces différences d'ordre technique ne devraient pas empêcher l'octroi de l'entraide. Dans les affaires auxquelles le critère de la double incrimination est applicable, il devrait l'être d'une façon souple, de nature à faciliter l'octroi de l'assistance.

153 RS **311.53**.

154 RS **0.311.55** ; voir ch. 260 du rapp. expl. (lien disponible sous note 1).

155 RS **0.351.12**.

156 La Partie destinataire n'est liée par la Partie d'envoi que dans la mesure où la Partie destinataire accepte l'information spontanée : en acceptant l'information, elle accepte également d'être tenue de respecter les conditions dont est assortie la transmission de ladite information. En ce sens, l'art. 26 de la Convention représente quelque chose qui est « à prendre ou à laisser ».

157 La criminalité ne s'arrête pas aux frontières et les informations récoltées par une Partie lors de ses investigations sont souvent susceptibles d'intéresser les autorités d'une autre Partie.

s'effectue conformément au droit national. En Suisse, l'art. 67*a* EIMP[158] en fixe les conditions.

2.3.6 Art. 27 - Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

L'art. 27 reprend des principes d'autres instruments dont la Suisse est partie. L'art. 27, par. 1, prévoit que l'entraide se déroule selon les conventions et traités d'entraide correspondants, comme la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959[159] ou son Deuxième Protocole additionnel précité. Les mécanismes d'entraide de criminalité informatique, fixés aux art. 29 à 35 de la Convention, supposent toutefois la mise en place de fondements juridiques si le droit applicable de l'Etat Partie concerné est insuffisant.

L'art. 27, par. 2 à 10, prévoit des règles régissant l'entraide en l'absence de traité, parmi lesquelles la création d'une autorité centrale, l'imposition de conditions, les motifs et procédures en cas d'ajournement ou de refus, la confidentialité des requêtes et les communications directes. Cette réglementation se substitue donc aux dispositions de droit interne. L'art. 27 ne règle pas d'autres questions[160].

L'art. 27, par. 2, de la Convention sur la cybercriminalité nécessite une communication de la Suisse au Secrétaire général du Conseil de l'Europe indiquant qui exercera la tâche d'autorité centrale chargée d'envoyer les demandes d'entraide ou d'y répondre en l'absence d'accord international. De même que concernant la déclaration émise en relation avec la CEEJ, il convient, en ce sens, de préciser que « l'Office fédéral de justice du Département fédéral de justice et police à Berne est compétent pour recevoir ou transmettre toutes les demandes d'entraide judiciaire émanant respectivement de l'étranger ou de la Suisse ». Lié à ce qui précède, l'art. 27, par. 9, let. e, autorise les Etats Parties à faire une déclaration énonçant que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale. En application de la présente disposition, les demandes devront être adressées à l'OFJ, ce qui suppose un surplus de travail et un besoin supplémentaire en personnel[161]. En effet, les demandes d'entraide adressées à l'OFJ en vertu de la Convention sur la cybercriminalité ne concerneront pas uniquement la répression d'infractions informatiques, mais également la récolte de preuves relatives à toutes autres infractions pénales détenues sous forme électronique[162]. Ce type de demandes d'entraide présente généralement un niveau de complexité supérieur aux demandes ordinairement soumises et nécessite un traitement prioritaire. En raison de la complexité de la matière, l'OFJ doit également s'attendre à être régulièrement consulté par les autorités suisses et étrangères, et donnera avis et conseils sur les procédures applicables. Cette mission d'information se doublera, lors de l'exécution de demandes d'entraide adressées à la Suisse, d'une

158 Transmission spontanée de moyens de preuve et d'informations.
159 CEEJ ; RS **0.351.1**.
160 Ainsi, par exemple, on n'y trouve aucune disposition concernant la forme et le contenu des requêtes, l'audition de témoins dans les Parties requise ou requérante, l'établissement de documents officiels, le transfert de témoins incarcérés ou l'assistance en matière de confiscation. En ce qui concerne ces questions, il découle de l'art. 25, par. 4, qu'en l'absence de disposition spécifique dans le présent chapitre, le droit interne de la Partie requise fixe les modalités de l'octroi de ce type d'entraide, donc pour la Suisse c'est l'EIMP qui s'applique. Voir ch. 264 du rapp. expl. (lien disponible sous note 1).
161 Dont service de piquet et formation idoine.
162 Art. 25, par. 1.

mission de contrôle accrue des décisions rendues par les autorités d'exécution suisses. En effet, en vertu du nouvel art. 18*b* EIMP[163], un certain nombre de décisions qui jusqu'ici pouvaient être attaquées par l'OFJ et par la personne touchée seront dorénavant soumises à l'unique contrôle de l'OFJ, garant de la crédibilité du système mis en place par cette disposition. Cette modification entraînera également l'obligation d'expliquer à l'autorité étrangère les conditions posées par l'art. 18*b* EIMP et de veiller à leur respect. Il conviendra d'établir, au sein de l'OFJ, un groupe de spécialistes du domaine de la cybercriminalité pour répondre aux exigences de la Convention. Ces compétences et responsabilités devraient nécessiter, en termes d'employés, l'équivalent d'un poste à temps complet supplémentaire, service de piquet compris. Ceci permettra à la Suisse d'assurer le type de riposte rapide si important dans la lutte contre la criminalité informatique ou en relation avec l'ordinateur. Les cantons devront aussi agir vite dans la lutte contre la criminalité selon la Convention et faire face à des besoins en spécialistes ainsi qu'en équipement informatique approprié.

L'art. 27, par. 3, oblige la Partie requise à exécuter les demandes conformément à la procédure spécifiée par la Partie requérante, à moins qu'elle soit incompatible avec sa législation. Une telle réglementation se trouve dans d'autres traités internationaux[164] et a pour but de pouvoir donner suite aux règles de preuve[165]. L'art. 27, par. 4, permet de refuser d'exécuter les demandes d'entraide : a) pour les motifs de l'art. 25, par. 4, de la Convention[166] ; b) pour l'infraction considérée par la Partie requise comme politique ou liée à une infraction politique et c) par le risque de porter atteinte à la souveraineté de l'État, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de la Partie requise[167]. L'art. 27, par. 5, clause habituelle, permet à la Partie requise d'ajourner, non de refuser, l'exécution d'une demande d'entraide si l'exécution immédiate des mesures visées par la demande risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités[168]. Selon l'art. 27, par. 6, dans les cas où elle serait normalement amenée à refuser ou ajourner sa coopération, la Partie requise peut l'assortir de conditions. Si celles-ci ne conviennent pas à la Partie requérante, la Partie requise peut les modifier, ou refuser sa coopération, ou y surseoir. L'art. 27, par. 7, de la Convention oblige la Partie requise à informer la Partie requérante de la suite qu'elle entend donner à sa

163 Présenté au ch. 2.3.9.1, « Nécessité de modifier le droit actuel ».

164 Notamment art. V de l'Accord du 10 septembre 1998 entre la Suisse et l'Italie en vue de compléter la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 et d'en faciliter l'application (RS **0.351.945.41)** et art. 9 du Traité du 25 mai 1973 entre la Confédération suisse et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale (RS **0.351.933.6)**.

165 Selon l'objectif d'assurer le respect des dispositions du droit interne régissant l'admissibilité des preuves dans l'Etat requis, afin de pouvoir utiliser lesdites preuves en justice, voir ch. 267 du rapp. expl. (lien disponible sous note 1).

166 C'est-à-dire les motifs prévus par le droit interne de la Partie requise.

167 Au nom du principe supérieur consistant à accorder l'entraide la plus large possible, les motifs de refus établis par une Partie requise doivent être limités et invoqués avec modération. Par conséquent, outre les motifs de refus visés à l'art. 28 de la Convention, le refus d'entraide au motif de la protection des données ne peut être invoqué que dans des cas exceptionnels. Voir ch. 268 et 269 du rapp. expl.

168 Ainsi, par exemple, si la Partie requérante a demandé la communication de preuves ou la déposition d'un témoin aux fins d'enquête ou de procès, et que les mêmes preuves ou dépositions sont nécessaires au déroulement d'un procès sur le point de commencer dans la Partie requise, celle-ci pourra valablement surseoir à l'exécution desdites mesures. Voir ch. 270 du rapp. expl.

demande d'entraide et de motiver tout refus ou ajournement de l'entraide[169]. Selon l'art. 27, par. 8, la Partie requérante peut demander à la Partie requise que le fait et l'objet de la requête restent confidentiels[170]. La Suisse a accepté une telle clause dans le Deuxième Protocole additionnel à la CEEJ[171].

L'art. 27, par. 9, institue une rapidité de communication : les autorités centrales selon l'art. 27, par. 2, communiquent directement entre elles. En cas d'urgence, les juges et procureurs de la Partie requérante peuvent cependant adresser les demandes d'entraide judiciaire directement à leurs homologues de la Partie requise, avec copie de la demande à l'autorité centrale de leur pays, à charge pour celle-ci de la transmettre à l'autorité centrale de la Partie requise. Les demandes peuvent être transmises par Interpol[172]. Les autorités de la Partie requise qui reçoivent une demande ne relevant pas de leur compétence doivent : a) transmettre la demande à l'autorité compétente de la Partie requise ; b) en informer les autorités de la Partie requérante[173]. Les demandes peuvent aussi être transmises directement, sans l'intervention des autorités centrales, même sans caractère d'urgence, si l'autorité de la Partie requise peut les exécuter sans mesures de coercition. Enfin, un Etat Partie peut informer les autres, par le Secrétaire général du Conseil de l'Europe, que, pour des raisons d'efficacité, les demandes doivent être adressées directement à son autorité centrale. Il en ira ainsi de la Suisse[174].

2.3.7 Art. 28 - Confidentialité et restriction d'utilisation

L'art. 28 prévoit des restrictions à l'utilisation d'informations ou de matériel afin de permettre à la Partie requise, lorsque ces informations ou ce matériel sont de nature particulièrement délicate, de s'assurer que leur utilisation est limitée à celle en vue de laquelle l'entraide est accordée. Comme l'art. 27 de la Convention, l'art. 28 ne s'applique que lorsqu'il n'existe pas d'instrument en vigueur entre les Parties requérante et requise[175]. L'art. 28, par. 2, permet à la Partie requise de fixer deux types de conditions : a) les informations ou le matériel fournis restent confidentiels

169 L'obligation faite à la Partie requise d'indiquer ses raisons a pour but d'améliorer l'efficacité de l'entraide et de permettre à la Partie requérante d'avoir accès à des informations factuelles dont elle n'avait pas eu connaissance concernant l'existence ou la situation de témoins ou de preuves. Voir ch. 272 du rapp. expl. (lien disponible sous note 1).

170 Il peut en effet arriver qu'une Partie fasse une demande d'entraide à propos d'une affaire très délicate ou d'une affaire pour laquelle la divulgation prématurée des faits ayant motivé la requête pourrait avoir des conséquences désastreuses. Toutefois, la confidentialité ne peut être sollicitée que dans la mesure où elle n'empêche pas la Partie requise d'obtenir les preuves ou les informations demandées. Il en irait ainsi, par exemple, si la divulgation des informations en question était indispensable pour obtenir une ordonnance judiciaire aux fins d'exécution de la demande d'entraide, ou qu'il faille notifier la requête à des particuliers ayant des preuves en leur possession pour que cette requête puisse être exécutée. Voir ch. 273 du rapp. expl.

171 La Partie requise ne pouvant faire droit à une demande de confidentialité en informe la Partie requérante, laquelle peut retirer sa demande ou la modifier.

172 Art. 27, par. 9, let. b.

173 Art. 27, par. 9, let. c.

174 Art. 27, par. 9, let. e, et cf. ci-dessus explications relatives à l'art. 27, par. 2.

175 Ceci sauf si lesdites Parties en décident autrement. On évite ainsi tout chevauchement avec des traités d'entraide judiciaire bilatéraux et multilatéraux existants et des arrangements analogues, ce qui permet aux praticiens de continuer d'appliquer le régime habituel au lieu de chercher à appliquer deux instruments concurrents pouvant, éventuellement, se révéler contradictoires, cf. ch. 276 du rapp. expl. (lien disponible sous note 1).

lorsque la demande ne pourrait être respectée sans cette condition[176] ; b) la communication d'informations ou de matériel ne servent pas aux fins d'autres enquêtes ou procédures que celles indiquées dans la requête. En Suisse, la règle de la spécialité de l'art. 67 EIMP est fondamentale dans la pratique : les documents et renseignements communiqués ne peuvent, dans l'Etat requérant, ni être utilisés aux fins d'investigations, ni produits comme moyens de preuve dans une procédure pénale visant une infraction pour laquelle l'entraide est exclue[177]. La restriction d'utilisation du matériel communiqué s'applique si elle est expressément demandée par la Partie requise; à défaut, la Partie requérante n'est pas tenue de la respecter. Cette restriction garantit que les informations et le matériel ne pourront être utilisés qu'aux fins prévues dans la demande, excluant qu'ils le soient à d'autres fins sans le consentement de la Partie requise. La Convention sur la cybercriminalité prévoit cependant deux exceptions à la capacité de restreindre l'utilisation des informations[178]. Si la Partie requérante ne peut satisfaire à l'une des conditions, elle en informe la Partie requise qui décide alors si elle va procurer les informations[179]. Il peut être demandé à la Partie requérante de communiquer des précisions quant à l'usage fait des informations ou du matériel reçus aux conditions énoncées au par. 2, de sorte que la Partie requise puisse vérifier que ces conditions ont été respectées[180]. En relation avec la règle de la spécialité de l'art. 67 EIMP précité, la Suisse sera parfois appelée à vérifier le respect des conditions dont la transmission est assortie.

2.3.8 Art. 29 - Conservation rapide de données informatiques stockées

L'art. 29, par. 1, autorise un Etat Partie à demander, et le par. 3 impose à chaque Etat Partie de se donner, les moyens juridiques d'obtenir la conservation rapide de données stockées au moyen d'un système informatique sur le territoire de la Partie requise, afin que ces données ne soient pas modifiées, enlevées ou effacées pendant la période nécessaire à la préparation, à la transmission et à l'exécution d'une demande d'entraide aux fins d'obtention des données. La conservation est une mesure provisoire limitée. En effet, les données informatiques sont des plus volatiles. Le présent mécanisme doit garantir la disponibilité de ces données pendant le déroulement du processus long et complexe de l'exécution d'une requête officielle d'entraide. Cette mesure est plus rapide et moins intrusive que la méthode d'entraide habituelle. A ce stade, il n'est pas demandé aux responsables de l'entraide de la Partie requise d'obtenir la possession des données auprès de leur gardien, mais il faut que la Partie requise s'assure que le gardien, qui est souvent un fournisseur de

176 Comme dans le cas de l'identité d'un informateur qui doit rester confidentielle, voir ch. 277 du rapp. expl. (lien disponible sous note 1).

177 Cette interdiction se rapporte notamment aux actes revêtant, selon la conception suisse, un caractère politique, militaire ou fiscal : cf. art. 3, sp. al. 1 et 3 EIMP : constitue un acte de caractère fiscal celui qui paraît à diminuer des recettes fiscales ou contrevient à des mesures de politique monétaire, commerciale ou économique. Toutefois, les documents et informations transmis par la voie de l'entraide peuvent aussi être utilisés pour la poursuite d'une escroquerie en matière fiscale.

178 a) si le matériel transmis constitue des éléments de preuve disculpant un accusé, il est révélé à la défense ou à une autorité judiciaire et b) si la plupart du matériel fourni dans le cadre des accords d'entraide est destiné à une utilisation lors de procès, souvent dans une procédure publique avec divulgation obligatoire ; une fois divulgué, ce matériel tombe pour l'essentiel dans le domaine public et il n'est pas possible de garantir la confidentialité aux fins d'enquêtes ou de procédures pour lesquelles l'entraide a été requise. Voir ch. 278 du rapp. expl.

179 Art. 28, par. 3.

180 Art. 28, par. 4.

services ou autre tiers, conserve, soit n'efface pas, les données en attendant que soit ordonnée leur remise ultérieure[181]. En droit suisse, cette exigence est remplie par les mesures provisoires que l'autorité d'exécution suisse compétente peut prononcer selon l'art. 18 EIMP. Ainsi, un fournisseur de service pourra être invité à effectuer sur un support séparé la sauvegarde (*backup*) des données intéressant les autorités étrangères, préservant ainsi celles-ci d'un effacement ultérieur, par leur utilisateur ou par le fournisseur de service. L'autorité étrangère sera amenée à présenter une demande d'entraide formelle dans un délai prescrit, faute de quoi la sauvegarde pourra être détruite. La procédure instituée à l'art. 29 de la Convention est rapide et respecte le droit de la personne concernée au respect de sa vie privée, car les données ne seront divulguées que lorsqu'il aura été satisfait aux critères applicables à la divulgation intégrale selon les accords d'entraide. La présente disposition permet d'engager un processus extrêmement rapide pour empêcher les données d'être perdues à jamais ; il s'agit de conservation des données en attendant leur remise ultérieure. Ces mesures ne sont toutefois concevables que si le fournisseur de service n'est pas lui-même impliqué dans les faits poursuivis à l'étranger, auquel cas les mesures provisoires devraient avoir lieu par le biais d'une perquisition.

L'art. 29, par. 2, énonce la teneur d'une telle demande de conservation. Cette mesure provisoire est préparée et transmise rapidement, les informations seront résumées et ne porteront que sur les éléments minimaux requis[182] pour permettre la conservation des données. La Partie requérante s'engage à soumettre ultérieurement une demande d'entraide pour obtenir la production des données.

La double incrimination n'est en principe pas requise comme condition préalable pour procéder à la conservation[183], car elle est contre-productive en matière de conservation[184]. Mais l'art. 29, par. 4 institue une réserve limitée. La Suisse l'émettra concernant la double incrimination, dans la mesure où cette dernière est nécessaire à notre pays pour toutes les mesures intrusives. La Suisse se réservera ainsi le droit, pour des infractions autres que celles établies conformément aux art. 2 à 11[185] de la Convention, de refuser la demande de conservation au titre de l'art. 29, par. 4, visant la perquisition ou l'accès similaire[186], la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées, dans le cas où notre pays aura des raisons de penser que, au moment de la divulgation, la condition de double

181 Voir ch. 282 du rapp. expl. (lien disponible sous note 1).

182 En sus de l'identification de l'autorité demandant la conservation et de l'infraction à l'origine de la demande, cette dernière fournit un bref exposé des faits, des indications suffisantes pour identifier les données à conserver et déterminer leur emplacement, et pour montrer le lien existant entre ces données et l'enquête ou la poursuite engagée au titre de l'infraction en question, ainsi que la nécessité de la mesure de conservation. Voir ch. 284 du rapp. expl. (lien disponible sous note 1).

183 Art. 29, par. 3.

184 En effet, la conservation n'est pas particulièrement intrusive dans la mesure où a) le gardien ne fait que maintenir la possession de données se trouvant légalement en sa possession et où b) les données ne sont divulguées aux responsables de la Partie requise ou examinées par eux qu'après l'exécution d'une demande d'entraide officielle visant leur divulgation.

185 La condition de la double incrimination est automatiquement remplie s'agissant des infractions établies conformément aux art. 2 à 11 de la Convention, sauf dispositions contraires figurant dans les réserves, prévues par la Convention, que les Parties peuvent avoir formulées au sujet de ces infractions. Par conséquent, les Parties ne peuvent imposer la condition de la double incrimination que concernant les infractions autres que celles qui sont définies dans la Convention.

186 Cf. la réserve correspondante de notre pays à la CEEJ.

incrimination ne pourra pas être remplie. La teneur de la réserve qui sera émise par la Suisse sera largement calquée sur celle présentée à l'appui de l'art. 5 CEEJ et sera formulée ainsi :

« La Suisse se réserve le droit de subordonner à la condition visée à l'art. 29, par. 4, l'exécution de toute commission rogatoire exigeant l'application d'une mesure coercitive quelconque. »

L'art. 29, par. 5, de la Convention fixe des conditions strictes au refus possible de la demande de conservation[187]. Dans leur application pratique, les art. 29 et 30 seront interprétés. En tant que mesures provisoires, ils précèdent une demande d'entraide formelle ; l'autorité étrangère peut exiger la conservation rapide selon l'art. 29 et la divulgation rapide selon l'art. 30. La Suisse procédera toutefois à une interprétation différenciée des art. 29, par. 5, et 30, par. 2: s'il apparaît, au moment d'ordonner les mesures provisoires, que la demande d'entraide tendant à la remise des données conservées sera irrecevable, la Suisse devrait refuser d'ordonner lesdites mesures provisoires. En effet, l'art. 31 permet d'exclure l'entraide selon le droit national et les traités. Donc si la Suisse ne donne pas suite à la demande d'entraide, il n'y a pas de raison qu'elle conserve les données relatives à une telle demande irrecevable.

Si la Partie requise se rend compte que le gardien des données risque de nuire à l'enquête[188], la Partie requérante doit être rapidement informée[189]. Elle pourra ainsi déterminer si elle prend le risque de l'exécution de la requête de conservation ou s'il vaut mieux utiliser une forme plus intrusive mais plus sûre d'entraide[190]. L'art. 29, par. 7, de la Convention impose que les données conservées le soient pour une période d'au moins 60 jours en attendant la réception de la demande d'entraide officielle visant leur divulgation et continuent d'être conservées après la réception de la demande, ce qui ne pose pas de problème en Suisse[191], dans la mesure où la loi ne fixe aucune durée minimale de conservation des données, celle-ci dépendant de la libre appréciation de l'autorité d'exécution, soumise au contrôle - et le cas échéant au recours - de l'OFJ.

2.3.9 Art. 30 - Divulgation rapide de données conservées

2.3.9.1 Nécessité de modifier le droit actuel

La révolution des technologies de l'information a radicalement changé la société. Elles se sont insinuées dans toutes les activités humaines par l'échange de vastes

187 La Partie requise ne peut refuser la demande de conservation que si son exécution risque de porter préjudice à sa souveraineté, sa sécurité, l'ordre public ou d'autres intérêts essentiels, ou si elle considère l'infraction comme étant de nature politique ou liée à une infraction de nature politique. L'efficacité de l'instruction et de la poursuite des infractions informatiques ou en relation avec l'ordinateur ont rendu cette mesure nécessaire, il a par conséquent été interdit de se prévaloir de tout autre motif pour refuser une demande de conservation, voir ch. 287 du rapp. expl.

188 Par exemple lorsque les données à conserver sont sous la garde d'un fournisseur de services contrôlé par une organisation criminelle ou par la cible de l'enquête elle-même.

189 Art. 29, par. 6.

190 Telle que l'injonction de produire ou la perquisition et la saisie. Voir ch. 288 du rapp. expl.

191 Voir ch. 289 du rapp. expl. (lien disponible sous note 1).

quantités de données[192]. Des changements économiques et sociaux sans précédent en sont la conséquence, mais de nouveaux types de délinquance sont aussi apparus. Les nouvelles technologies bousculent les principes juridiques existants et nécessitent des mesures techniques de protection des systèmes informatiques et des mesures juridiques de prévention de la délinquance et de dissuasion. Dans ce domaine, la rapidité de la transmission des informations recueillies conditionne l'efficacité de la lutte contre le crime. A l'inverse des moyens de preuves ordinaires, qui se caractérisent par une certaine durabilité dans le temps et dans l'espace[193] et ne souffrent pas de procédures durant plusieurs mois, les données informatiques peuvent transiter entre différents pays de manière quasiment instantanée et ne font généralement pas l'objet de stockage durable, celui-ci dépassant rarement quelques mois. La seule prise de mesures provisoires rapides (saisie des données intéressantes) est insuffisante ; ces mesures doivent se doubler d'une transmission des données aussi diligente que possible à l'autorité requérante, faute de quoi elles s'avéreront inexploitables. Cet impératif fait l'objet de l'art. 30 de la Convention.

Or, le droit suisse en vigueur ne satisfait pas à la mise en œuvre de l'art. 30 de la Convention. Il arrive souvent qu'à la demande d'un Etat Partie dans lequel une infraction a été commise, la Partie requise conserve les données relatives au trafic concernant la transmission d'une communication par ses ordinateurs afin de pouvoir remonter à la source de la communication et identifier l'auteur de l'infraction, ou localiser des preuves décisives. Ce faisant, la Partie requise peut s'apercevoir que les données relatives au trafic découvertes sur son territoire montrent que la communication a été acheminée par un fournisseur de services d'un Etat tiers ou par un fournisseur se trouvant dans la Partie requérante elle-même. En pareil cas, la Partie requise doit fournir rapidement à la Partie requérante une quantité suffisante de données relatives au trafic pour permettre d'identifier le fournisseur de services de l'Etat tiers et la voie par laquelle la communication a été transmise par celui-ci. Si la communication a été transmise depuis un Etat tiers, ces informations permettent à la Partie requérante d'adresser à ce dernier une demande de conservation et d'entraide accélérée pour identifier le fournisseur de services et la voie de transmission de la communication. L'art. 30 nécessite de pouvoir divulguer rapidement les données relatives au trafic à l'étranger, données accessibles grâce à un ordre de surveillance émis selon la LSCPT. Cette obligation est peu compatible avec le système d'entraide suisse actuel qui nécessite, avant toute transmission à l'étranger d'éléments relatifs au domaine secret[194], la notification à leur titulaire d'une décision de clôture susceptible de recours[195]. Ce n'est qu'à l'issue de cette procédure, qui dure plusieurs mois, que les données peuvent être transmises à l'autorité étrangère. Ce délai entraîne que les données s'avèrent inexploitables par l'autorité étrangère, car trop anciennes, et permet en outre aux personnes concernées, averties par les autorités

192 La facilité avec laquelle il est possible d'avoir accès à l'information contenue dans les systèmes informatiques et la consulter a, couplée aux possibilités pratiquement illimitées d'échange et de diffusion de cette information, par delà les distances géographiques, déclenché une explosion de l'information disponible et des connaissances qui peuvent en être tirées.

193 Par exemple, la banque est tenue de conserver pendant dix ans la documentation relative à la tenue de ses comptes.

194 Art. 9 EIMP et art. 69 de la loi fédérale sur la procédure pénale (RS **312.0)**.

195 Art. 80*e* EIMP. Une telle procédure n'est pas nécessaire lorsque la communication investiguée constitue elle-même une infraction commise par Internet. Dans ce cas, le fournisseur de services a l'obligation de transmettre toutes les informations permettant d'identifier l'auteur selon une procédure simplifiée (art. 14, al. 4, LSCPT).

suisses, de faire disparaître[196] les moyens de preuves compromettants. Sur ce point, le droit suisse doit donc être adapté pour répondre aux exigences de l'art. 30, ce qui fait l'objet du nouvel art. 18*b*, al. 1, let. a, ci-après, disposition qui couvre également, à son al. 1, let. b. les besoins de la mise en œuvre de l'art. 33:

> ***Art. 18b Données relatives au trafic informatique***
>
> *[1] L'autorité fédérale ou cantonale chargée de traiter une demande d'entraide peut ordonner la transmission à l'étranger de données relatives au trafic informatique avant la clôture de la procédure d'entraide lorsque :*
>
> *a. les mesures provisoires font apparaître que la source de la communication faisant l'objet de la demande d'entraide se trouve à l'étranger, ou que*
>
> *b. ces données sont recueillies par l'autorité d'exécution en vertu d'un ordre de surveillance en temps réel qui a été autorisé (art. 269 à 281 du code de procédure pénale du 5 octobre 2007).*
>
> *[2] Ces données ne peuvent pas être utilisées comme moyen de preuve avant que la décision sur l'octroi et l'étendue de l'entraide n'ait acquis force de chose jugée.*
>
> *[3] La décision prévue à l'al. 1 et, le cas échéant, l'ordre et l'autorisation de surveillance sont immédiatement communiqués à l'office fédéral.*

Le nouvel art. 18*b* autorise la transmission des données (relevant du domaine secret) relatives au trafic à l'autorité étrangère avant la clôture de la procédure d'entraide dans deux situations : a) les mesures provisoires font apparaître que la source de la communication faisant l'objet de la demande d'entraide se trouve à l'étranger (al. 1, let. a : législation d'application de l'art. 30 de la Convention) ; b) ces données sont recueillies par l'autorité d'exécution en vertu d'un ordre de surveillance en temps réel qui a été autorisé (al. 1, let. b : législation d'application de l'art. 33 de la Convention). Une telle transmission déroge au système actuel de l'entraide, raison pour laquelle la personne touchée bénéficie d'une protection juridique accrue instituée à l'art. 18*b*, al. 2 et 3, dans l'éventualité d'un refus ultérieur de l'entraide. Ces mesures de protection sont de trois ordres :

a) la mesure de surveillance doit recueillir l'autorisation d'un tribunal indépendant au sens de l'art. 272 CPP (cf. nouvel art. 18*b*, let. b in fine, EIMP);
b) les données transmises ne peuvent pas être utilisées comme moyens de preuve avant la clôture de la procédure, ce qui permet, en cas de recours admis, de faire écarter du dossier étranger les informations communiquées (cf. nouvel art. 18*b*, al. 2, EIMP); et
c) cette transmission est soumise au contrôle immédiat de l'OFJ (cf. nouvel art. 18b, al. 3, EIMP).

196 L'existence de risques de disparition des preuves constitue une circonstance justifiant le recours à une transmission immédiate ; tel est, par exemple, le cas lorsque l'autorité étrangère recherche l'identité d'une personne utilisant des services Internet suisses pour échanger des fichiers de pédopornographie. Actuellement, les données permettant d'identifier l'utilisateur d'un tel service ne peuvent pas être transmises à l'autorité étrangère avant que l'utilisateur n'ait été informé de la décision rendue à son égard et n'ait bénéficié d'un délai de trente jours pour recourir contre cette décision, délai qui lui permet de faire disparaître de son ordinateur personnel toutes les données compromettantes.

Seules pourront être transmises les données recueillies selon un ordre de surveillance autorisé. Ceci garantit que les données ont été récoltées conformément au droit suisse et que la demande d'entraide a été examinée non seulement par l'autorité d'exécution, mais également par un magistrat indépendant[197]. Ce contrôle est encore accru par le fait que toute décision de transmission doit être immédiatement annoncée à l'OFJ à qui il incombera de veiller au respect de la loi et qui, en cas d'abus ou d'irrespect de cette disposition, pourra intervenir tant auprès des autorités suisses qu'étrangères. La présente disposition revêt un certain caractère de nouveauté dans le système de l'entraide suisse, car elle autorise la transmission à l'autorité étrangère de renseignements relevant du domaine secret sans que la personne concernée ait été préalablement avertie et ait eu l'occasion de faire valoir ses arguments. Une telle transmission est nécessaire pour remplir les exigences de la Convention qui tient compte des impératifs de la poursuite pénale. Cette disposition diminue la possibilité de la personne touchée de se défendre immédiatement contre la transmission à l'étranger d'éléments relevant de son domaine secret. La protection dont la personne touchée bénéficie reste toutefois assurée par d'autres mécanismes. En effet, la demande d'entraide sera non seulement examinée par l'autorité d'exécution mais également, de manière accrue, par l'OFJ. De plus, l'autorité autorisant la surveillance[198] devra également vérifier que la demande remplit un certain nombre de critères, recoupant étroitement, sur un plan matériel, ceux de la procédure d'entraide[199]. La personne touchée n'est pas privée de tous ses droits : dès que la situation le permettra[200], elle devra être avertie de la transmission intervenue et pourra recourir non seulement contre la décision de clôture, mais également contre la décision de surveillance. Si elle obtient gain de cause, l'autorité étrangère devra retirer ces informations de son dossier et en donner quittance aux autorités suisses. Dans tous les cas, jusqu'à ce que la personne touchée ait pu faire valoir ses droits, les informations la concernant ne pourront pas être utilisées à titre de preuves, mais uniquement à titre d'investigation[201]. Le système proposé tient ainsi compte d'une manière raisonnable des impératifs de la poursuite pénale tout en assurant que les intérêts légitimes de la personne touchée continuent de bénéficier d'une protection adéquate. Enfin, la présente modification sera également utile en matière d'extradition, pour la localisation des suspects.

D'un point de vue formel, l'autorité compétente saisie d'une demande tendant à la surveillance en temps réel de données relatives au trafic devra rendre une décision d'entrée en matière et requérir les éventuelles autorisations nécessaires selon l'art. 272 CPP. Dans la même décision, ou par décision incidente séparée, l'autorité d'exécution ordonnera également la transmission anticipée et sous conditions des

197 Bien que l'examen de ce magistrat ne porte pas sur l'entraide proprement dite, il recouvre en grande partie les critères essentiels utilisés en entraide.

198 Art. 7, al. 1, LSCPT.

199 Il en est ainsi de la double incrimination (qualifiée selon l'art. 3 LSCPT), de la proportionnalité (subsidiarité des mesures: art. 3, al. 1, let. a à c, LSCPT) ainsi que du tri des documents (art. 8 LSCPT).

200 Mais dans tous les cas au plus tard lors de la clôture de la procédure pénale ou de la suspension de la procédure (art. 10, al. 2, LSCPT).

201 Voir sur cette distinction le message du Conseil fédéral du 1er octobre 2004 concernant l'art. 30 de l'Accord de coopération entre la Confédération suisse, d'une part et la Communauté européenne et ses États membres, d'autre part, pour lutter contre la fraude et toute autre activité illégale portant atteinte à leurs intérêts financiers, FF **2004** 5820. Le même critère est également utilisé en droit suisse, voir par ex. art. 10, al. 3, LSCPT et art. 22 de la loi fédérale du 20 juin 2003 sur l'investigation secrète (LFIS).

données obtenues en vertu de l'ordre de surveillance. Cette décision devra être immédiatement transmise à l'OFJ qui pourra recourir[202], si les conditions légales ne sont pas réalisées. L'ordre et l'autorisation de surveillance seront également communiqués à l'OFJ, afin que celui-ci puisse contrôler que les conditions de l'art. 18*b* sont réalisées.

En ce qui concerne les mesures de surveillance en temps réel, elle doivent, par essence, rester inconnues des personnes surveillées. Dans la coopération internationale, ce postulat se concilie difficilement avec le principe de base de l'EIMP, selon lequel aucune information relevant de la sphère secrète d'une personne ne peut être transmise à l'étranger sans que celle-ci n'ait préalablement eu la possibilité de s'y opposer. Ces intérêts divergents ne se limitent toutefois pas à la seule transmission de données relatives au trafic, qui fait l'objet de l'art. 33 de la Convention, mais concernent également la transmission des contenus de communications surveillées en temps réel. Ce conflit potentiel a été reconnu par la doctrine qui relève les problèmes actuels liés à l'exécution de demandes d'entraide relatifs à la surveillance en temps réel de télécommunications[203]. La révision se limite toutefois à ce que la mise en œuvre de l'art. 33 requiert, s'étendant uniquement aux données relatives au trafic, sans inclure celles relatives au contenu. L'art. 18*b* EIMP ne crée donc pas de régime légal unique autorisant l'exécution de mesures de surveillance dans le cadre de l'entraide judiciaire et concernant les données relatives au trafic ainsi que celles relatives au contenu.

Les autres développements relatifs au nouvel art. 18*b*, let. b, EIMP sont présentés à l'appui de l'art. 33 de la Convention.

2.3.9.2 Autres développements relatifs à l'art. 30

Selon l'art. 30, par. 2, la Partie requise ne peut refuser la divulgation de données relatives au trafic que si celle-ci risque de porter préjudice à sa souveraineté, sa sécurité, son ordre public ou d'autres intérêts essentiels, ou si elle considère l'infraction comme politique ou liée à une infraction politique. Comme pour l'art. 29 de la Convention, ce type d'informations est si important pour pouvoir identifier les auteurs d'infractions ou localiser des preuves décisives que les motifs de refus de divulgation ont été limités[204].

2.3.10 Art. 31 - Entraide concernant l'accès aux données stockées

L'art. 31 prévoit que chaque Etat Partie a la capacité, au bénéfice de l'autre, de perquisitionner ou d'accéder par un moyen similaire, de saisir ou d'obtenir par un moyen similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur son territoire, tout comme il a, en vertu de l'art. 19[205] de la Convention, celle de le faire à des fins nationales[206]. Le fait que l'art. 31 ne permet pas de restreindre les mesures prévues à une catégorie particulière d'infractions et qu'aucune réserve ne puisse être formulée[207] n'apparaît pas

202 Art. 80*e*, 80*h* et 80*l* EIMP.
203 Thomas Hansjakob, BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St-Gall 2006; Robert Zimmermann, La coopération judiciaire internationale en matière pénale, Berne, 2004, n. 246-13 ss, p. 285 ss.
204 Voir ch. 291 du rapp. expl.
205 Perquisition et saisie de données informatique stockées.
206 Voir ch. 292 du rapp. expl.
207 Art. 42.

problématique, car l'art. 31 est exécuté en application des traités applicables et du droit national mentionné à l'art. 23 de la Convention.

L'art. 31, par. 1, autorise une Partie à demander le type d'entraide prévu par la présente disposition et le par. 2 exige de la Partie requise qu'elle se donne les moyens de la fournir. Selon l'art. 31, par. 2, cette coopération est fournie aux conditions des traités, arrangements et législations nationales applicables. L'art. 31, par. 3, prévoit qu'il est satisfait rapidement à une telle demande lorsque : a) il y a des raisons de penser que les données pertinentes sont particulièrement susceptibles de perte ou de modification, ou que b) les traités, arrangements ou législations prévoient une coopération rapide[208].

2.3.11 Art. 32 - Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

L'art. 32 règle l'accès, par un Etat Partie, aux données stockées dans un autre Etat, plus précisément aux données accessibles au public[209] et dans le cas où la personne légalement autorisée à divulguer les données y consent. Il s'agit donc de cas où un Etat agit unilatéralement mais où il est admis qu'il n'y a pas atteinte à la souveraineté de l'autre Etat[210]. La disposition crée le cadre juridique de ces deux cas d'accès à des données stockées dans un autre Etat sans l'accord de ce dernier[211]. Il n'a pas été possible, lors des négociations, de parvenir à un consensus sur une règlementation plus étendue.

Pour ce qui est des données accessibles au public (par ex. des données disponibles sur le site Internet d'une entreprise), l'art. 32 permet à un Etat Partie de les télécharger et de les utiliser sans être tenu de requérir l'accord de l'Etat dans lequel se trouvent ces données. Il lui permet aussi de consulter ou de se procurer des données se trouvant dans un autre Etat lorsqu'une personne légalement autorisée à lui divulguer ces données lui donne son consentement légal et volontaire. S'il s'agit d'informations confidentielles sur une tierce personne qui n'a pas donné son accord pour qu'elles soient publiées, l'accès unilatéral prévu par l'art. 32 n'est pas autorisé.

Cette disposition de la Convention doit être interprétée de manière étroite, notamment dans le deuxième cas prévu, car il faut éviter qu'elle ne soit utilisée pour éluder la procédure d'entraide judiciaire ou pour violer la sphère privée d'un tiers[212]. Le droit légal qu'a une personne de disposer de données et de les transmettre à une administration étatique est régi en tout premier lieu par la législation de l'Etat où elle agit. Il est ainsi permis d'enregistrer son courrier électronique auprès d'un fournisseur de services étranger et de le transmettre à une autorité de son propre Etat[213]. Concrètement, une personne se trouvant à l'étranger qui a enregistré des données en Suisse pourra toujours les fournir volontairement à une administration étrangère sans en informer les autorités suisses, dans la mesure où elle y est

208 Voir ch. 292 du rapp. expl. (lien disponible sous note 1).
209 Source ouverte.
210 Voir ch. 293 du rapp. expl (cf. note 1).
211 Et sans recours à la voie ordinaire de l'entraide judiciaire ou administrative. La Convention n'autorise aucun autre accès de ce type ; cf. art. 39, par. 3, de la Convention.
212 L'Allemagne a suivi cette optique en mettant en œuvre la Convention. Cf. le commentaire du projet de loi du gouvernement fédéral allemand du 16 novembre 2007 relatif à la Convention sur la cybercriminalité, Drucksache 16/7218, p. 55, consultable à l'adresse http://dip21.bundestag.de/dip21/btd/16/072/1607218.pdf.
213 Des données peuvent être stockées à l'étranger sans que l'ayant droit le sache, parce que le fait n'est pas apparent.

légalement autorisée et où elle ne porte pas atteinte au domaine secret protégé d'un tiers.

2.3.12 Art. 33 - Entraide dans la collecte en temps réel de données relatives au trafic

L'art. 33 impose de collecter en temps réel des données relatives au trafic pour un autre Etat Partie et de coopérer en la matière. Les clauses et conditions concernant l'octroi de cette coopération sont celles que prévoient les traités et législations applicables régissant l'entraide judiciaire pénale. En effet, souvent les enquêteurs ne peuvent être sûrs de pouvoir remonter à la source d'une communication en se fiant aux enregistrements des transmissions antérieures, car des données relatives au trafic cruciales peuvent avoir été automatiquement effacées par un fournisseur de services de la filière de transmission avant de pouvoir être conservées. Il est donc indispensable que les enquêteurs de chaque Etat Partie puissent avoir la possibilité de se procurer en temps réel des données relatives au trafic concernant des communications transmises par un système informatique se trouvant sur le territoire d'autres Etats Parties[214]. Certes, l'art. 33, par. 2, permet que l'entraide ainsi fournie équivale au moins aux « infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne ». Selon le droit actuel, les données relatives au trafic relèvent du domaine secret, sont récoltées de manière secrète et nécessitent une décision de clôture avant d'être transmises. Le nouvel art. 18*b* EIMP présenté au ch. 2.3.9.1 permet de transmettre immédiatement ces données à l'étranger, notamment sans procéder à une notification de la décision[215] à la personne concernée en Suisse, ce qui, par conséquent, ne met pas non plus l'enquête étrangère en danger.

Il convient de préciser que l'art. 33 de la Convention ne prévoit pas de limitation quant à la gravité de l'infraction justifiant l'application des mesures de surveillance ; or, le nouvel art. 273[216] CPP autorisera la surveillance en temps réel des données relatives au trafic uniquement pour des enquêtes en relation avec des délits et des crimes. L'art. 15, par. 2, de la Convention sur la cybercriminalité prévoit cependant que les pouvoirs et procédures doivent « intégrer le principe de proportionnalité », chaque Etat Partie appliquant ce principe selon les autres principes de son droit interne[217]. Les Etats Parties à la Convention peuvent donc ne pas donner suite à une demande ne respectant pas ce principe de proportionnalité, ce qui permettrait à la Suisse de refuser sa coopération lorsque les faits constituent une contravention selon le droit suisse. La question des paris en lignes, lesquels peuvent générer des sommes très importantes, pourrait s'avérer délicate, dans la mesure où ces derniers constituent une contravention au sens du droit suisse[218].

214 Voir ch. 295 du rapp. expl. (lien disponible sous note 1).
215 Art. 80*m* EIMP.
216 Le nouveau droit procédural pénal autorisera une surveillance rétroactive si la gravité de l'infraction la justifie et si elle apparaît nécessaire à l'instruction (art. 273, al. 1, let. b et c, CPP), même si cette infraction n'est pas mentionnée dans le catalogue de l'art. 269 CPP.
217 Voir ch. 146 du rapp. expl.
218 Art. 42 de la loi fédérale du 8 juin 1923 sur les loteries et les paris professionnels (LLP ; RS **935.51)**.

2.3.13 Art. 34 - Entraide en matière d'interception de données relatives au contenu

L'art. 34 restreint l'obligation d'accorder l'entraide aux fins d'interception des données relatives au contenu en raison du caractère très intrusif de l'interception. Cette entraide est accordée dans la mesure permise par les traités et lois internes applicables. La pratique de l'entraide en la matière n'en est qu'à ses débuts, donc les régimes et législations internes d'entraide déterminent l'étendue de l'obligation de coopérer et des restrictions dont cette obligation fera l'objet[219]. Au sens du nouvel art. 18*b* EIMP proposé sous ch. 2.3.9.1, seules les données relatives au trafic informatique peuvent être communiquées à l'étranger avant la clôture d'une procédure. Les données relatives au contenu ne peuvent pas l'être. Donc, selon l'art. 30, al. 1 EIMP[220], les autorités suisses ne pourront pas demander à l'étranger de collecter en temps réel des données relatives au contenu.

2.3.14 Art. 35 - Réseau 24/7

En vertu de l'art. 35 de la Convention, les Etats Parties veillent à ce qu'un point de contact soit joignable en tout temps. Ce point de contact est chargé de faciliter les investigations pénales nationales et internationales concernant la cybercriminalité. Il ne doit pas impérativement prendre lui-même des mesures dans les domaines du conseil juridique, de l'entraide judiciaire, de l'administration des preuves, de la conservation des données ou des enquêtes pénales en général[221]. La seule exigence de la Convention est qu'il serve d'intermédiaire voué à faciliter les relations entre les autorités suisses et étrangères chargées de ces tâches.

Cette fonction pourra être assumée par la Centrale d'engagement de l'Office fédéral de la police (fedpol). C'est l'OFJ (service de piquet) qui remplira les tâches relatives à l'entraide judiciaire et à l'extradition prévues à l'art. 35, par. 1, let. a à c, de la Convention (et qui tranchera notamment sur l'admissibilité des mesures).

Il est difficile de chiffrer la charge supplémentaire que représentera l'exécution des cas d'entraide judiciaire et des demandes dans le domaine couvert par la Convention sur la cybercriminalité. Cela dépendra du nombre d'Etats Parties à la Convention, de la complexité des cas et des développements technologiques utilisés d'une part par les délinquants et d'autre part par les autorités de poursuite pénale[222]. On estime qu'un poste à plein temps sera nécessaire à l'OFJ du fait de la ratification et de la mise en œuvre de la Convention (piquet et traitement ordinaire des cas). Du côté de fedpol, dont la Centrale d'engagement, dépendant de la Police judiciaire fédérale, recevra des annonces 24 h/24 et devra établir et faciliter le contact avec les autorités compétentes, un poste à plein temps sera également nécessaire.

Les services concernés de fedpol considèrent cependant qu'il serait souhaitable de prévoir davantage de ressources, au-delà de ce qu'exige la Convention. Ils préconisent, afin de mieux tirer profit de l'instauration du point de contact, de le doter d'un large spectre de tâches qui ne font pas partie des exigences minimales de

219 Voir ch. 297 du rapp. expl. (lien disponible sous note 1).
220 Les autorités suisses ne peuvent adresser à un Etat étranger une demande à laquelle elles ne pourraient pas donner suite en vertu de la présente loi.
221 Cf. art. 35, par. 1, de la Convention et ch. 298 ss du rapp. expl. (lien disponible sous note 1).
222 Ressources et équipements dans les domaines de la surveillance, de la sécurité et du contrôle du trafic de données électroniques.

la Convention. Notamment, ce nouveau service pourrait apporter un appui technique et juridique immédiat à l'accomplissement des tâches mentionnées à l'art. 35, par. 1, let. a à c, de la Convention. Il pourrait également établir les contacts et mettre en route les processus nécessaires aux interactions entre les autorités de poursuite pénale et les fournisseurs de services Internet, favorisant la rapidité et l'efficacité de la poursuite pénale[223].

La coopération des fournisseurs de services Internet avec les autorités de poursuite pénale requiert des échanges constants entre les acteurs impliqués et la mise en place de formations techniques et juridiques. Si telles étaient les tâches – extensives – du point de contact qu'il faut créer, elles seraient à rattacher, administrativement et matériellement, au Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)[224], organe chargé de soutenir la Confédération et les cantons dans ce domaine, qui possède déjà un réseau de contacts avec les enquêteurs IT des polices cantonales et avec divers fournisseurs Internet. Il faudrait à cet effet adjoindre au SCOCI deux postes (estimation dans l'état actuel des connaissances) pour utiliser au mieux les synergies[225].

Il serait également approprié d'instaurer un service de piquet au Commissariat Enquêtes Technologie de l'information de la Police judiciaire fédérale, afin d'assurer un soutien rapide aux procédures d'entraide judiciaire et aux procédures pénales relevant du domaine fédéral. Le commissariat pourrait aussi fournir davantage de soutien aux autorités de poursuite cantonale, dont l'expertise dans le domaine de la cybercriminalité, nécessaire en vue de l'entraide judiciaire et de manière générale dans les enquêtes portant sur les technologies de l'information, est inégale. Ces tâches requerraient selon toute estimation deux postes supplémentaires.

La question des ressources que le Parlement devra approuver et d'une éventuelle compensation au sein du Département fédéral de justice et police sera examinée dans le message.

2.4 Chapitre IV: Clauses finales

Les clauses finales de la Convention correspondent peu ou prou à celles d'autres conventions du Conseil de l'Europe.

Selon son *art. 36*, la Convention est ouverte à la signature non seulement des Etats membres du Conseil de l'Europe, mais aussi des Etats non membres qui ont participé à son élaboration[226]. D'autres Etats peuvent être invités à y adhérer[227].

La Convention est entrée en vigueur le 1er juillet 2004, une fois que cinq Etats l'ont eu ratifiée[228]. Aujourd'hui, elle compte 23 Etats Parties. Parmi eux, seuls les Etats-Unis ne sont pas membres du Conseil de l'Europe.

223 Cf. les lignes directrices du Conseil de l'Europe pour la coopération entre organes de répression et fournisseurs de services internet contre la cybercriminalité, consultables à l'adresse http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp.

224 http://www.cybercrime.ch.

225 En raison de l'organisation de la SCOCI, ces deux postes ne pourraient pas lui être intégrés, mais ils devraient lui être rattachés administrativement.

226 L'Afrique du Sud, le Canada, les Etats-Unis et le Japon.

227 *Art. 37* de la Convention. Y ont été invités, à ce jour (novembre 2008), le Costa Rica, le Mexique et les Philippines.

228 Art. *36, par. 3*, de la Convention.

Nous l'avons dit plus haut : la possibilité de remettre des déclarations et des réserves a été expressément prévue comme partie intégrante à la Convention lors de l'élaboration de celle-ci[229]. L'*art. 40* énumère les six dispositions de la Convention concernant lesquelles les Etats Parties peuvent émettre une restriction. Nous proposons que la Suisse dépose des déclarations relatives aux art. 2, 3, 7, 9, ch. 3, et 27, ch. 9, let. e, (pour davantage de détails voir le commentaire de ces dispositions).

En vertu de l'*art. 41* (Clause fédérale), un Etat peut déclarer par une réserve qu'il ne se soumettra pas aux obligations visées au chapitre II[230] en raison de sa structure fédérale[231], à condition que le domaine de la coopération internationale[232] n'en soit pas touché. Pour la Suisse, cette option ne présente pas d'intérêt puisque le CPP, qui entrera bientôt en vigueur, confie à la Confédération la compétence en matière de droit de procédure.

La Convention présente une particularité : elle limite la possibilité de faire des réserves, l'*art. 42* donnant la liste des dispositions qui peuvent en faire l'objet. Il est prévu que la Suisse fasse quatre réserves, relatives aux art. 6, ch. 3, 9, ch. 4, 14, ch. 3, et 29, ch. 4. Nous renvoyons ici aussi au commentaire de ces dispositions.

Les réserves et déclarations comprises dans l'avant-projet d'arrêté fédéral devront être adressées au Secrétaire général du Conseil de l'Europe en même temps que la Suisse déposera les instruments de ratification.

Tout différend sur l'interprétation ou l'application de la Convention doit être réglé en premier lieu par la négociation (*art. 45*). Contrairement à d'autres conventions récentes du Conseil de l'Europe, celle-ci ne connaît pas de mécanisme réciproque de surveillance ou d'évaluation.

La Convention peut être dénoncée à tout moment, moyennant un délai de trois mois, par notification au Secrétaire général du Conseil de l'Europe (*art. 47*).

2.5 Protocole additionnel du 28 janvier 2003 contre les actes de nature raciste et xénophobe

Le Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, du 28 janvier 2003, enjoint aux Etats Parties d'ériger en infraction pénale la discrimination et l'incitation à la haine et à la violence sur la base de la race, de la couleur, de l'ascendance, de l'origine ou de la religion de la victime. Il déclare applicables à ces infractions les dispositions de la Convention sur la cybercriminalité. Le Protocole est entré en vigueur le 1er mars 2006 et a été ratifié par treize Etats, dont trois de l'UE.

La Suisse l'a signé le 9 octobre 2003. Le droit suisse correspond aux exigences impératives du Protocole. Bien que la norme pénale sur le racisme (art. 261bis CP) ne mentionne pas les critères de la couleur, de la descendance et de l'origine nationale, ils sont couverts de fait par ceux de l'appartenance raciale et ethnique.

229 Voir ch. 49 et 50 du rapp. expl. (lien disponible sous note 1).
230 Mesures à prendre au niveau national.
231 Une clause inhabituelle, qui a été reprise dans le texte en raison de l'intervention déterminante des Etats-Unis.
232 Chapitre III de la Convention.

Le droit suisse en vigueur va plus loin que le Protocole sur plusieurs points. Ainsi, il considère la religion comme un critère en soi ; de même, il ne réduit pas le concept de l'ethnie à l'origine ethnique, ce qui peut avoir des implications considérables dans les faits.

Bien que notre droit soit largement compatible avec le Protocole, nous proposons de ratifier seulement la Convention. La mise en œuvre du Protocole, qui concerne une matière tout autre, devrait être examinée dans un deuxième temps, afin qu'il soit possible de se concentrer sur les questions matérielles de la criminalité informatique, de la procédure pénale dans le domaine des preuves électroniques et de l'entraide judiciaire. En outre, il vaut mieux attendre les résultats des travaux en cours au Département fédéral de justice et police concernant la punissabilité de l'utilisation de symboles racistes[233] pour pouvoir en tenir compte lorsque l'on examinera l'opportunité de mettre en œuvre le Protocole.

2.6 Rapport avec d'autres révisions du domaine du droit pénal

Le 5 octobre 2007, les Chambres fédérales ont adopté le code de procédure pénale qui est destiné à remplacer les codes cantonaux et la procédure pénale fédérale. Il devrait entrer en vigueur le 1er janvier 2011. Nous nous sommes référés à ses dispositions à plusieurs reprises dans le présent rapport[234], lorsqu'elles étaient importantes pour la mise en œuvre de la Convention sur la cybercriminalité et qu'elles permettaient de répondre aux exigences de celles-ci. L'entrée en vigueur de la Convention pour la Suisse demande donc que le CPP soit en vigueur. Il n'est pas probable qu'il prenne du retard.

Un groupe de travail de la Confédération a entrepris une révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication. Si des interférences entre les deux projets apparaissaient, la coordination est assurée.

3 Conséquences

3.1 Conséquences pour la Confédération en matière de finances et de personnel

Vu la multiplication des cas de cybercriminalité, il est prévisible que les autorités de poursuite pénale et le service chargé de la surveillance de la correspondance par poste et télécommunication, rattaché au Département fédéral de justice et police, seront plus sollicités de manière générale, indépendamment de la ratification de la Convention sur la cybercriminalité. Comme les cas liés à Internet ont pour la plupart des aspects internationaux, les services qui traitent les demandes d'entraide judiciaire seront aussi plus chargés.

La mise en œuvre et la ratification de la Convention est susceptible de représenter une lourde charge, sur les plans quantitatif et qualitatif, pour le service de l'OFJ compétent en matière d'entraide judiciaire. Quant à la Centrale d'engagement de la

233 Cf. le document de travail de l'OFJ de mai 2007 pour l'audition concernant la norme pénale sur le racisme, qui peut être consulté à l'adresse http://www.bj.admin.ch/bj/fr/home/themen/kriminalitaet/gesetzgebung/rassismus.html.

234 Cf. notamment le commentaire des art. 16 à 21, 23, 25, 30 et 33 de la Convention.

Police judiciaire fédérale, elle aura une nouvelle tâche de coordination. La question des ressources que devra approuver le Parlement et d'une éventuelle compensation au sein du Département fédéral de justice et police sera examinée dans le message.

3.2 Conséquences économiques

La mise en œuvre de la Convention n'aura aucune conséquence pour l'économie.

3.3 Conséquences en matière informatique

La mise en œuvre de la Convention n'aura pas de conséquences en matière informatique. L'équipement actuel des autorités de poursuite pénale de la Confédération, du Tribunal fédéral et du Tribunal pénal fédéral répond aux exigences de la Convention et est suffisant pour assurer la poursuite et l'évaluation des cas de cybercriminalité.

3.4 Conséquences pour les cantons

Vu l'essor des nouvelles technologies de communication et la rapidité avec laquelle elles transforment notre société, les cas de cybercriminalité sont appelés à se multiplier. Toutefois, la seule mise en œuvre de la Convention aura sans doute peu de conséquences pour les cantons. En particulier, il n'est guère à craindre que le nombre de poursuites pénales ou de cas d'entraide judiciaire concernant des infractions visées par la Convention augmente considérablement[235]. De plus, le point de contact exigé par la Convention sera intégré à fedpol et les demandes d'entraide judiciaire et de renseignements en la matière seront adressées à l'OFJ.

4 Rapport avec le programme de la législature

Le projet est annoncé dans le message sur le programme de la législature 2007-2011[236].

5 Aspects juridiques

5.1 Relation avec l'Union européenne

La mise en œuvre de la Convention ne présente pas de problèmes de compatibilité avec le droit de l'UE. Un petit nombre de pays membres de l'UE a déjà ratifié la Convention, plusieurs autres sont en train de la transposer dans leur droit national.

5.2 Constitutionnalité

L'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité repose sur l'art. 54, al. 1, de la Constitution (Cst.)[237], qui habilite la Confédération à conclure des traités internationaux. L'art. 184, al. 2, Cst. habilite le Conseil fédéral à conclure et ratifier les traités internationaux, lesquels sont, selon l'art. 166, al. 2, Cst., approuvés par l'Assemblée fédérale.

Les traités internationaux sont sujets au référendum s'ils sont d'une durée indéterminée et ne sont pas dénonçables, s'ils prévoient l'adhésion à une organisation internationale ou s'ils contiennent des dispositions importantes fixant des règles de droit ou que leur mise en œuvre exige l'adoption de lois fédérales[238].

235 Voir ch. 1.3 du présent rapport (appréciation de la Convention).
236 FF **2008** 639.
237 RS **101**.
238 Art. 141, al. 1, let. d, Cst.

La Convention sur la cybercriminalité est d'une durée indéterminée, mais elle est dénonçable en tout temps et ne prévoit pas l'adhésion à une organisation internationale. Néanmoins sa ratification implique de modifier le code pénal et la loi sur l'entraide pénale internationale. L'arrêté fédéral sera donc sujet au référendum facultatif en matière de traités internationaux prévu par l'art. 141, al. 1, let. d, ch. 3, Cst.

Les modifications de loi proposées se fondent sur les art. 54, al. 1, et 123, al. 1, Cst.

Annexe

Arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité (avant-projet)