TCVS P1 10 41

Droit pénal – Criminalité sur Internet, pornographie – ATC (Juge de la Cour pénale II) du 9 mars 2011, Ministère public c. X. – TCV P1 10 41

Criminalité sur Internet, pornographie

– Compétences du service de coordination de la lutte contre la criminalité sur Internet (SCOCI); distinction entre l'activité de monitoring et celle consistant à surveiller des réseaux de télécommunications dans le cadre d'une instruction pénale; en l'espèce, l'activité du collaborateur du SCOCI ne nécessitait aucune autorisation judiciaire préalable; la perquisition, intervenue avant l'ouverture formelle de l'instruction, n'est, par ailleurs, pas illégale (art. 13 al. 1 Cst., 2 LSCPT, 3 aLSCPT, 27 al. 1 let. a OSCPT, 2 ch.1, 41bis, 53 ss aCPP; consid. 5).

– N'est pas punissable l'utilisateur d'un logiciel de pair-à-pair configuré de manière à ce que les autres utilisateurs ne puissent pas accéder aux données téléchargées ou en cours de téléchargement (art. 197 ch. 1 CP; consid. 6a).

– En l'espèce, condamnation de l'auteur pour avoir téléchargé des vidéos de nature pédopornographique au moyen d'un logiciel et pour avoir gravé, sur des DVD, des vidéos de même nature (art. 197 ch. 3 al. 1 CP; consid. 6b).

Réf. CH: art. 13 Cst., art. 197 CP, art. 2 LSCPT, art. 3 aLSCPT, art. 27 OSCPT

Réf. VS: art. 2 aCPP, art. 41bis aCPP, art. 53 aCPP

Internetkriminalität, Pornographie

– Zuständigkeiten der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK); Unterscheidung zwischen Monitoring und der Überwachung des Fernmeldenetzes im Rahmen einer strafrechtlichen Untersuchung; vorliegend bedurfte der Mitarbeiter der KOBIK für seine Tätigkeit keiner vorgängigen richterlichen Bewilligung; die vor der formellen Eröffnung der Untersuchung durchgeführte Hausdurchsuchung ist ausserdem nicht illegal (Art. 13 Abs. 1 BV, 2 BÜPF, 3 aBÜPF, 27 Abs. 1 lit. a VÜPF, 2 Ziff 1, 41bis, 53 ff. aStPO; E. 5).

– Die Verwendung eines Peer-to-Peer-Systems, das so konfiguriert ist, dass andere Benutzer keinen Zugriff haben auf Inhalte, die heruntergeladen wurden oder gerade heruntergeladen werden, ist nicht strafbar (Art. 197 Ziff. 1 StGB; E. 6a).

– Verurteilung wegen Herunterladens kinderpornographischer Videos mit Hilfe eines Peer-to-Peer-Systems und wegen Speicherns solcher Videos auf DVD (Art. 197 Ziff. 3 Abs. 1 StGB; E. 6b).

Ref. CH: Art. 13 BV, Art. 197 StGB, Art. 2 BÜPF, Art. 3 aBÜPF, Art. 27 VÜPF

Ref. VS: Art. 2 aStPO, Art. 41bis aStPO, Art. 53 aStPO

Faits (extraits)

4. a) aa) Le 12 février 2007, X. a téléchargé sur son ordinateur personnel (alors connecté à Internet par l'adresse IP [Internet Protocol] dynamique 00.00.000.0), dont il est l'unique utilisateur, au moyen du logiciel eMule, via le réseau eDonkey, deux fichiers intitulés respectivement «(Yamad)Hussyfan!!New!!Childrens-Cam(Good!).avi» et «Dee.and.Desi.zadoom.pedo.cumshot.9.(1).mpg.» Selon les extraits

imprimés figurant au dossier, sur la première de ces vidéos, on peut voir une jeune fille de moins de 16 ans exhibant ses seins, nue, et les jambes écartées avec son sexe en gros plan, ainsi qu'une personne introduisant un doigt dans le sexe ou l'anus d'une jeune fille. Le second de ces fichiers montre un homme éjaculant sur le visage d'une jeune fille de moins de 16 ans.

bb) EMule est un logiciel libre et gratuit d'échange de tous types de fichiers informatiques (vidéo, audio, logiciels, etc.) au moyen du système pair-à-pair (peer-to-peer; en abrégé: P2P). Celui-ci permet à ses utilisateurs de transférer directement des fichiers entre eux sans passer par un serveur. Dans cette mesure, il est qualifié de décentralisé: chaque internaute devient un émetteur de fichiers à partager pour les autres utilisateurs, qui deviennent à leur tour des émetteurs de ces fichiers stockés sur leur propre ordinateur (Seeger, Identification des diffuseurs de fichiers illégaux dans les réseaux de partage de fichiers «peer-to-peer», in Cimichella/Kuhn/Niggli [édit.], Nouvelles technologies et criminalité: nouvelle criminologie?, 2006, p. 269). Autrement dit, les fichiers à télécharger ne sont pas proposés par l'éditeur du logiciel mais par chaque utilisateur qui les met à disposition sur son propre disque dur (dans un dossier ou un répertoire dit «partagé») auquel les autres utilisateurs peuvent accéder (Gilliéron, Propriété intellectuelle et Internet, 2003, p. 316, n^{os} 389 et 392). Le recours à ce mode de transfert nécessite l'utilisation d'un logiciel (tel qu'eMule) répertoriant tous les fichiers que les utilisateurs entendent partager. Ce logiciel, pourvu généralement d'une interface utilisateur conviviale, fait essentiellement office de moteur de recherche (Tirelli, La répression des consommateurs de pédopornographie à l'heure de l'Internet, thèse, Lausanne 2008, n° 46). Tout d'abord, il effectue une recherche sur la base d'un ou de plusieurs mots-clés sur l'un des serveurs communautaires et obtient un nombre variable de réponses décrivant la disponibilité du fichier recherché, c'est-à-dire le nombre de sources, ainsi que de multiples informations telles que le nom du fichier, sa taille, son type et son format informatique (MP3, MPEG, AVI, etc.). Chaque source correspond à un ordinateur détenant le fichier en question dans son répertoire partagé. Ensuite, l'utilisateur choisit un ou plusieurs des fichiers proposés et demande sa mise en téléchargement par un simple clic. Il obtient ainsi du serveur la liste et l'adresse IP des internautes émetteurs (Seeger, op. cit., p. 277). Une particularité des logiciels de P2P réside en ce que les fragments de données sont, pendant leur téléchargement même, automatiquement mis à la disposition des autres utilisateurs (Schwarzenegger, Urheberstrafrecht und Filesharing in

P2P-Netzwerken – Die Strafbarkeit der Anbieter, Downloader, Verbreiter von Filesharing-Software und Hash-Link-Setzer, in Schwarzenegger/Arter/Jörg [édit], Internet-Recht und Strafrecht, 2005, p. 213 et 220). Il est toutefois possible de configurer certains de ces programmes de manière à bloquer le partage automatique des données téléchargées (arrêt du TC/GR PS 06 5 du 27 juillet 2006 consid. 3a, reproduit in sic! 2008 p. 205 ss ; Schwarzenegger, op. cit., p. 220 et 228 ; Koller, Cybersex, Die strafrechtliche Beurteilung von weicher und harter Pornographie im Internet unter Berücksichtigung der Gewaltdarstellungen, thèse, Zurich 2007, p. 41).

cc) Aux termes de l'arrêt de renvoi du 24 mars 2010, pour «télécharger les fichiers litigieux, X. a dû faire une recherche incluant au moins l'un des mots du titre de ces fichiers, puis choisir, au vu des titres proposés, de les télécharger. Il a aussi pu décider de télécharger tous les fichiers répondant aux mots-clés choisis. Dans le premier cas, X. a décidé volontairement de télécharger des fichiers contenant la représentation d'actes d'ordre sexuel avec des enfants (au vu des titres de ces fichiers). Dans le second cas, il en a accepté le risque (au vu des mots-clés révélateurs qu'il a dû choisir)».

L'appelant prétend avoir uniquement entré dans le moteur de recherche les termes «cam» et «cumshot», et affirme qu'il ignorait tout du caractère pédopornographique des fichiers considérés.

En l'espèce, la question de savoir quels mots-clés l'intéressé a introduits dans le moteur de recherche d'eMule n'apparaît pas décisive. Au vu de l'intitulé explicite des fichiers litigieux («Hussyfan» associé à «Children» ; «pedo» associé à «cumshot»), il ne pouvait en effet qu'avoir conscience que ceux-ci comportaient des actes d'ordre sexuel impliquant des mineurs de moins de 16 ans. Il a d'ailleurs reconnu, lors des débats de première instance et d'appel, qu'il connaissait la signification du mot «cumshot» (éjaculation). Par ailleurs, certains des termes composant les fichiers téléchargés par X. («Hussyfan!!New!!», «pedo», «Children») se retrouvent dans le nom de plusieurs vidéos – aux titres à connotation ouvertement pédopornographique – qui avaient été effacées mais dont la trace, parmi celles de centaines d'autres, a été retrouvée sur le disque dur de son ordinateur personnel. Il apparaît donc exclu qu'il ait pu télécharger par mégarde les fichiers en question. Il y a d'autant moins lieu d'hésiter sur ce point que l'appelant, qui a fréquenté les cours de l'école d'informatique de Sierre, dispose de très bonnes connaissances en la matière. Dans ces circonstances, en sélectionnant et en cliquant sur les résultats obtenus par le moteur de recherche, X. a, à tout le moins à titre éventuel, accepté de télécharger

sur son ordinateur des vidéos illustrant des actes d'ordre sexuel avec des mineurs de moins de 16 ans.

L'appelant fait également valoir que le logiciel dont il s'est servi permettait de «bloquer les émissions» de sorte que les fichiers litigieux n'étaient pas accessibles aux autres utilisateurs.

En l'occurrence, on peut se demander si la version du logiciel eMule utilisée par X. pouvait être configurée de telle manière à empêcher tout partage automatique des données téléchargées ou en cours de téléchargement (cf. Koller, op. cit., p. 294 sv.). Selon la lettre du SCOCI du 10 avril 2007, l'appelant était «en train de télécharger [les fichiers] ou les avait déjà intégralement sauvegardés dans la zone libérée pour l'échange de données. Les fragments des films téléchargés sont immédiatement mis à disposition à d'autres utilisateurs d'Internet pour le téléchargement». Cette assertion de l'autorité dénonciatrice n'est toutefois corroborée par aucun élément matériel du dossier. Le juge d'instruction n'a fait procéder à aucun mesure d'investigation sur cette question; il n'a d'ailleurs pas ouvert d'instruction contre l'appelant ni ne l'a inculpé du chef de l'art. 197 ch. 1 CP. L'expert judiciaire ne s'est pas davantage prononcé à cet égard. Dans ces conditions, le juge de céans n'est pas en mesure de retenir que X. a permis à des tiers – notamment à des mineurs de moins de 16 ans – d'accéder aux fichiers pédopornographiques qu'il a téléchargés.

b) Les 30 avril et 16 août 2006, X. a gravé sur 4 DVD, dénommés respectivement «Teen Town 6 & 7», «Teen Test 5», «Girl Power» et «Harald Fick Show 5», des vidéos, d'une durée totale de 41 minutes et 37 secondes, représentant des actes d'ordre sexuel avec des mineurs de moins de 16 ans et des scènes d'urolagnie. L'accusé a reconnu la nature de ces vidéos et a admis avoir visionné une partie d'entre elles.

Considérants (extraits)

5. a) Dans un grief d'ordre formel, l'appelant fait valoir que le SCOCI «n'a pas le droit d'espionner eMule» et que, partant, les preuves recueillies par celui-ci sont entachées de nullité. Les objets saisis à son domicile par la police le 9 mai 2007 seraient en outre le fruit d'une perquisition illégale.

b) aa) La création du SCOCI repose sur un accord administratif conclu à la fin de l'année 2001 entre le Département fédéral de justice et police (DPFJ) et la conférence des chefs des départements cantonaux de justice et police (CCDJP), visant à autoriser la Confédération à assumer des tâches d'information et de coordination dans le domaine de la criminalité sur Internet. Elle laisse subsister la compétence des

cantons en matière de poursuite des infractions, sous réserve de celles dont la poursuite ressortit à la juridiction fédérale (arrêt 6B_211/2009 du 22 juin 2009 consid. 1.1; Kronig/Bollmann, Die Koordinationstelle zur Bekämpfung der Internetkriminalität (KOBIK), in Schwarzenegger/Arter/Jörg, p. 30 ss). Le SCOCI est rattaché à l'Office fédéral de la police (fedpol; cf. art. 10 al. 1 let. h de l'ordonnance du 17 novembre 1999 sur l'organisation du Département fédéral de justice et police – RS 172.213.1). Il exerce des tâches de monitoring (recherches actives dans le but de déceler les infractions commises via Internet, premier traitement des communications de soupçons venant de la Suisse et de l'étranger, clarification et analyse des emplacements et de la paternité des contenus incriminés sur Internet, etc.), de clearing (examen du contenu pénal des messages entrants, coordination des procédures en cours, transmission des dossiers aux autorités de poursuite pénale) et d'analyse (analyse systématique et interprétation des sources internes et publiques dans le domaine de la criminalité sur Internet, analyse régulière de la situation en Suisse et information sur les tendances et les contre-mesures en la matière, etc.), domaines qui sont rattachés au service d'analyse et de prévention (SAP). Dans cette mesure, les agents du SCOCI, qu'il soient ou non des policiers au sens strict, interviennent alors comme employés d'un organisme étatique rattaché à une autorité de police, dont la mission spécifique est de contribuer à la lutte contre la criminalité via Internet, en exerçant des tâches équivalant à des investigations préliminaires de la police. En pareil cas, il faut donc considérer qu'ils accomplissent une activité assimilable à celle des fonctionnaires de police (arrêt 6B_211/2009 précité, eod. loc.).

Il convient de faire le départ entre l'activité de monitoring telle que décrite ci-dessus et celle consistant à surveiller des réseaux de télécommunications dans le cadre d'une instruction pénale. La première se déroule en effet dans l'espace public (öffentlicher Raum) et porte sur la partie d'Internet en principe accessible à tous; il s'agit donc principalement d'«observer» l'activité et le comportement des internautes dans le but de constater la commission d'infractions pénales, comme le ferait une patrouille de police dans le monde réel (Kronig/Bollmann, op. cit., p. 45 et 48; cf., ég., ATF 134 IV 266 consid. 3.9). Dès lors, le monitoring ne requiert pas le prononcé de mesures de contrainte et n'est partant pas subordonné à une autorisation judiciaire préalable (Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2006, p. 56; cf., ég., Rapport de la commission d'experts «Cybercriminalité», DFJP, Berne,

juin 2003, p. 82, ndp 183). La surveillance (Überwachung) d'Internet se rapporte en revanche aux données concernant la vie privée et familiale d'une personne soupçonnée d'avoir commis une infraction pénale, son domicile, sa correspondance et les relations qu'elle établit par la poste et les télécommunications (cf. art. 13 al. 1 Cst.), telles que, par exemple, le contenu de ses e-mails ou la teneur d'une conversation sur une chatroom «privée», par Instant Messenger ou Skype (Kronig/Bollmann, op. cit., p. 48). Avant le 1er janvier 2011, les mesures de surveillance d'Internet étaient soumises aux anciens art. 3 ss de la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT; Hansjakob, loc. cit.; Kronig/Bollmann, op. cit., p. 45; actuellement: art. 269 ss CPP). Leur prononcé ressortissait au juge d'instruction et devait être approuvé par le président de l'autorité de plainte du Tribunal cantonal (art. 6 et 7 aLSCPT; art. 103c ss aCPP).

bb) Il a été retenu en fait que l'appelant a téléchargé les fichiers litigieux au moyen du logiciel eMule, via le réseau eDonkey. Il s'agit d'un réseau P2P public et accessible sans mot de passe (cf. Kronig/Bollmann, op. cit., p. 45, ndp 52) à n'importe quelle personne disposant du programme – libre et gratuit – eMule. Par ailleurs, contrairement à ce que semble penser l'appelant, sur ce type de réseau, l'adresse IP de l'utilisateur n'est pas cachée aux autres internautes (cf. Seeger, op. cit., p. 277). Cela étant, l'intervention du collaborateur du SCOCI a simplement consisté, en l'espèce, à se connecter au réseau eDonkey et, dans un premier temps, à observer le comportement des différents utilisateurs en ligne. Ce collaborateur a ensuite constaté que l'utilisateur dont l'adresse IP était 00.00.000.0, correspondant à un raccordement d'un fournisseur d'accès sis en Valais – information qui est aussi librement disponible sur Internet (cf., par ex., http://www.ip-adress.com/ip_tracer) –, avait téléchargé plusieurs fichiers à contenu pédopornographique, soit des agissements pouvant tomber sous le coup de l'art. 197 CP. Dans cette mesure, il s'agit d'une pure tâche de monitoring entrant précisément dans les compétences susdécrites du SCOCI et ne nécessitant, par conséquent, aucune autorisation judiciaire préalable. Le collaborateur considéré n'a pas non plus investigué sur la toile en tant qu'«agent infiltré», de sorte que l'ancienne loi sur l'investigation secrète (LFIS) ne trouve pas à s'appliquer en l'occurrence (cf. ATF 134 IV 266). Au surplus, en tant qu'organe de police rattaché à fedpol, le SCOCI ne saurait être assimilé à une société privée telle que Logistep AG, qui poursuit un but purement économique (cf. ATF 136 II 508 consid. 6.3.1). Enfin, le nom et l'adresse de l'appelant ont été valablement communiqués par le fournisseur d'accès à l'autorité compétente en la

matière, à savoir le service des tâches spéciales (STS), alors rattaché au Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC; cf. art. 2 LSCPT et 27 al. 1 let. a OSCPT; Hansjakob, n. 2 ad art. 27 OSCPT).

Il suit des développements qui précèdent que le grief de l'appelant relatif à la nullité des preuves recueillies par le SCOCI est infondé. Il en va de même de celui pris de l'illégalité de la perquisition effectuée par la police à son domicile le 9 mai 2007. Cette mesure, ainsi que, notamment, la saisie de son l'ordinateur et de plusieurs DVD, se fondent en effet sur le mandat écrit délivré par le magistrat instructeur le 24 avril 2007 (cf. art. 2 ch. 1 et 41bis ch. 1 aCPP; Piquerez, Traité de procédure pénale suisse, 2006, nos 897 sv.). Il est certes vrai que celui-ci n'a formellement ouvert une instruction contre X. du chef de pornographie que le 16 mai 2007 et que l'art. 45bis aCPP ne permet pas au juge d'instruction, sauf péril en la demeure, de procéder à des mesures coercitives dans le cadre de l'enquête préliminaire. Cette irrégularité n'a toutefois aucune incidence sur les actes accomplis par la police le 9 mai 2007. Elle implique uniquement que l'ouverture matérielle de l'instruction est intervenue le 9 mai 2007 et qu'à partir de cette date déjà, l'appelant revêtait la qualité de partie à la procédure avec les droits qui y sont rattachés, notamment celui de consulter le dossier, de participer aux actes d'instruction et de requérir des opérations (art. 53 ss aCPP; ATC P3 09 50 du 30 avril 2009; cf., ég., RVJ 2002 p. 297 consid. 2a). Or, en l'espèce, il n'apparaît pas que X. aurait été entravé dans l'exercice de ces prérogatives.

6. a) L'art. 197 ch. 1 CP punit d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire celui qui aura offert, montré, rendu accessibles à une personne de moins de 16 ans ou mis à sa disposition des écrits, enregistrements sonores ou visuels, images ou autres objets pornographiques ou des représentations pornographiques, ou les aura diffusés à la radio ou à la télévision. Le premier juge a correctement exposé les conditions d'application de cette disposition ainsi que sa portée à la lumière de la jurisprudence et de la doctrine, de sorte que l'on peut s'y référer. Il convient d'y ajouter que n'est pas punissable celui qui prend des mesures efficaces pour empêcher que des mineurs de moins de 16 ans puissent accéder à l'objet ou à la représentation pornographique (ATF 131 IV 64 consid. 10.1.2; Corboz, Les infractions en droit suisse, 2010, n. 27 ad art. 197 CP; Meng/Schwaibold, Commentaire bâlois, n. 32 ad art. 197 CP; Koller, op. cit., p. 163). Tel est en particulier le cas de l'utilisateur d'un logiciel de P2P configuré de manière à ce que les autres utilisateurs ne puissent pas accéder aux

données téléchargées ou en cours de téléchargement (cf. Koller, op. cit., p. 296).

En l'espèce, le juge de céans n'a pas été en mesure de retenir que X., en téléchargeant les deux fichiers litigieux, les a rendus accessibles – c'est-à-dire téléchargeables – à d'autres utilisateurs d'eMule, parmi lesquels pouvaient se trouver des mineurs de moins de 16 ans. En de telles occurrences, l'appelant ne peut qu'être acquitté du chef d'accusation de pornographie au sens de l'art. 197 ch. 1 CP.

b) Aux termes de l'art. 197 ch. 3 al. 1 CP, celui qui aura fabriqué, importé, pris en dépôt, mis en circulation, promu, exposé, offert, montré, rendu accessibles ou mis à la disposition des objets ou représentations visés au ch. 1, ayant comme contenu des actes d'ordre sexuel avec des enfants, des animaux, des excréments humains ou comprenant des actes de violence, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. S'agissant des conditions d'application de cette disposition, le juge de céans se réfère aux considérations pertinentes du jugement entrepris.

Il a été circonscrit en fait que, le 12 février 2007, X. a téléchargé sur son ordinateur personnel au moyen du logiciel eMule deux vidéos montrant des actes d'ordre sexuel avec des mineurs de moins de 16 ans. Au vu des noms respectifs des deux fichiers en question, l'appelant, en cliquant sur les résultats obtenus au moyen du moteur de recherche d'eMule, a, à tout le moins à titre éventuel, accepté de télécharger sur le disque de son ordinateur des vidéos de nature pédopornographique. Il est en outre constant que, les 30 avril et 16 août 2006, X. a gravé sur 4 DVD, dénommés respectivement «Teen Town 6 & 7», «Teen Test 5», «Girl Power» et «Harald Fick Show 5», des vidéos, d'une durée totale de 41 minutes et 37 secondes, représentant des actes d'ordre sexuel avec des mineurs de moins de 16 ans et des scènes d'urolagnie (ou urophilie). L'accusé a admis la nature de ces vidéos et concédé avoir visionné une partie d'entre elles. Partant, il doit être reconnu coupable de pornographie au sens de l'art. 197 ch. 3 CP.