BStGer BG.2012.27 vom 4. Oktober 2012

Bundesstrafgericht, 2012-10-04, FR

Quelle: https://mcp.opencaselaw.ch/entscheid/bstger_BG.2012.27

FR: TPF BG.2012.27 du 4 octobre 2012

IT: TPF BG.2012.27 del 4 ottobre 2012

Regeste

Compétence ratione materiae (art. 28 CCP).

Erwägungen

E. 1.1

Le pouvoir de la Cour des plaintes du Tribunal pénal fédéral de connaître des litiges entre le MPC et les autorités cantonales de poursuite pénale portant sur la compétence d'enquêter en matière de criminalité économi- que, au sens de l'art. 24 al. 1 CPP, résulte de l'art. 28 CPP en lien avec l'art. 37 al. 1 LOAP. En pareil cas, l'autorité de céans statue selon les rè- gles que la loi et la jurisprudence ont fixées pour la résolution des conflits de for intercantonaux (SCHWERI/BÄNZIGER, Interkantonale Gerichtsstands- bestimmung in Strafsachen, 2ème éd., Berne 2004, no 419 et le renvoi à l'ATF 128 IV 225 consid. 2.3; v. également TPF 2011 170 consid. 1.1 et ar- rêt du Tribunal pénal fédéral BG.2009.20 du 28 septembre 2009, consid. 1.1). La saisine de la Cour des plaintes présuppose qu'existe une contesta- tion relative à la compétence pour connaître d'une affaire, d'une part, et que les parties aient procédé à un échange de vues à ce propos, d'autre part (SCHWERI/BÄNZIGER, op. cit., nos 561 et 599; GUIDON/BÄNZIGER, Die ak- tuelle Rechtsprechung des Bundesstrafgerichts zum interkantonalen Ge- richtsstand in Strafsachen, in Jusletter du 21 mai 2007, [no 4]). S'agissant du délai dans lequel l'autorité requérante doit saisir la Cour de céans, il a été décidé de s'en tenir aux dix jours prévus à l'art. 396 al. 1 CPP, excep- tion faite du cas dans lequel l'autorité requérante invoque des circonstan- ces exceptionnelles qu'il lui incombe de spécifier (v. TPF 2011 94 consid. 2.2). Les autorités habilitées à représenter leur canton dans le cadre de l'échange de vues, puis durant la procédure devant l'autorité de céans, sont déterminées par le droit de procédure propre à chaque canton (art. 14 al. 4 CPP; v. à ce sujet KUHN, in Basler Kommentar, Schweizerische Straf- prozessordnung, 2011, no 9 ad art. 39 CPP, et no 10 ad art. 40 CPP; SCHMID, Handbuch des schweizerischen Strafprozessrechts, Zurich/Saint- Gall 2009, no 488; GALLIANI/MARCELLINI, Codice svizzero di procedura pe- nale [CPP] - Commentario, Zurich/Saint-Gall 2010, no 5 ad art. 40 CPP).

E. 1.2

La demande de fixation de compétence matérielle ayant été déposée dans le délai mentionné plus haut (v. supra consid. 1.1), et les parties ayant été représentés par des autorités légitimées à le faire, il y a lieu d'entrer en ma- tière sur le fond de la cause.

E. 2.1

La réalisation des conditions de la poursuite pénale et l'absence d'empê- chements de procéder sont nécessaires pour qu'une autorité se saisisse d'une affaire et mène une procédure. La compétence matérielle, à raison du lieu et fonctionnelle sont des conditions procédurales dites "positives" (HAUSER/SCHWERI/HARTMANN, Schweizerisches Strafprozessrecht, 6ème éd., Bâle 2005, p. 179 nos 13 s.). Dites conditions doivent être examinées d'office, à chaque stade de la procédure (KIPFER, in Basler Kommentar, Schweizerische Strafprozzessordnung, 2011, no 5 ad Intro art. 22-28 CPP). La délimitation des compétences entre cantons et Confédération est réglée aux art. 22 à 28 CPP. Selon l'art. 22 CPP, les autorités pénales cantonales disposent d'une compétence de principe puisqu'elles sont compétentes pour la poursuite et le jugement des infractions prévues par le droit fédéral, sous réserve des exceptions prévues par la loi. Ces exceptions figurent aux art. 23 et 24 CPP.

E. 2.2

A teneur de l’art. 24 al. 1 CP, la juridiction fédérale est notamment compé- tente pour connaître des infractions aux art. 260ter et 305bis CP si les ac- tes punissables ont été commis pour une part prépondérante (en allemand: "für einen wesentlichen Teil"; en italien: "prevalentemente") à l’étranger, ou dans plusieurs cantons, sans qu’il y ait de prédominance évidente dans l’un d’entre eux. L'art. 24 CPP reprend, sans modifications majeures, le contenu de l'art. 337 aCP, lequel avait pour sa part remplacé l'art. 340bis aCP, de sorte que la jurisprudence et la doctrine relatives à ces dispositions conser- vent toute leur valeur. Les compétences de la Confédération en lien avec ces infractions ont pour prémisse la volonté du législateur d'améliorer la lut- te contre la criminalité internationale (BERTOSSA, in Commentaire romand, Code de procédure pénale suisse, 2011, no 2 ad art. 24 CPP). Selon la ju- risprudence, la question de savoir si l’une ou l’autre des infractions visées à l’art. 24 al. 1 let. a CPP a été commise "pour une part prépondérante à l’étranger" doit être résolue en des termes qualitatifs et non quantitatifs. L'infraction doit être considérée comme ayant été commise pour une part prépondérante à l'étranger si sa composante étrangère atteint une "masse critique" telle que les nouveaux moyens d'enquête mis à disposition de la Confédération apparaissent mieux adaptés que les moyens cantonaux pour assurer une répression efficace du crime (ATF 130 IV 68 consid. 2.2 in fine). La compétence de la Confédération découlant de l'art. 24 al. 1 CPP est impérative, à la différence de celle rattachée à l'alinéa second de cette disposition. La jurisprudence rendue en lien avec la question de la compé- tence impérative de la Confédération montre que les contours de cette der- nière demeurent, dans une large mesure, difficiles à préciser. Il en va no- tamment ainsi du critère de rattachement de l'organisation criminelle dont

traite l'art. 260ter CP, et à propos duquel il n'est souvent pas possible, en début d'enquête, de savoir si le crime provient d'une telle organisation (v. ATF 132 IV 89 consid. 2). La délimitation des compétences entre autori- tés de poursuite pénale de la Confédération et celles des cantons ne dé- pend pas de ce qui pourra finalement être imputé à l'accusé. Elle doit plutôt s'opérer sur la base des soupçons existant au moment où la question doit être tranchée (ATF 133 IV 235 consid. 4.4).

E. 2.3.1

Dans le cas d'espèce, le dossier soumis à la Cour de céans permet de re- tenir ce qui suit:

Le dénommé B., citoyen péruvien domicilié au Pérou, a ouvert, le 6 mars 2012, un portefeuille "virtuel-électronique" auprès de la société A. SA, dont le siège est à Fribourg. Il a par la suite utilisé plus d'une centaine de re- charges D.-card provenant du monde entier pour créditer ce portefeuille. Une fois ces montants crédités, l'intéressé a commencé à procéder à leur rapatriement vers un compte bancaire dont il est le titulaire auprès de la banque C. au Pérou.

Les agissements de l'intéressé ont attiré l'attention de l'intermédiaire finan- cier, lequel a demandé des justifications sur les transferts en question. En l'absence d'une réponse satisfaisante, A. SA a dénoncé le cas au MROS, en indiquant ce qui suit:

"Le client a utilisé plus d'une centaine de recharges D.-card provenant du monde entier. Lorsque nous avons demandé à notre client de nous fournir une copie des 3 dernières D.-card utilisées sur A. SA, il nous a transmis de fausses cartes et n'a pas été en mesure d'expliquer la provenance des avoirs. (…). Le client semble exploiter une plateforme d'échange de cartes prépayées, ce qui est interdit par D. Sàrl (…)".

Il ressort encore du dossier que D. Sàrl, le 17 avril 2012, a adressé à la so- ciété A. SA un courriel à la teneur suivante:

"Dear business partner,

We kindly ask for your cooperation with this email. For several months we have been fighting together with law enforcement agencies against a cy- bercrime organization that uses a "Trojan" virus to extort ransom to be paid with D.-card vouchers in order to unblock victims' computers. The or-

ganization causes significant damage to thousands of customers and D. Sàrl itself.

The Trojan works by initially infecting the customer's PC through some "drive-by" websites, which act as infection points. Then, the customer's PC is locked and the customer is prompted to provide credentials (PIN-Code) of a D.-card, mostly to the value of 100 EUR. Once the cybercrime gang is in possession of the D.-card PIN it typically sells the PIN code at a dis- count of up to 60% via illegal online E-currency exchange platforms. The platforms, which have been identified but are hosted and operated outside of jurisdictions that prosecute such activities, are best discribed as han- dling stolen goods. (…)." (act. 1.8, p. 16 s.).

Des transactions frauduleuses du type mentionné ci-dessus auraient été constatées sur la relation d'affaires dont dispose B. auprès de la société A. SA.

Se fondant sur l'ensemble de ces informations, le MROS a procédé à des recherches dans ses bases de données. Il en résulte que B. n'est pas connu des autorités suisses pour des faits en relation avec le blanchiment d'argent et ne figure dans aucun registre judiciaire suisse. Le MROS, dans sa communication au MPC du 4 mai 2012, précise toutefois que:

"(…) l'affaire dénoncée par l'intermédiaire financier, mentionnant la possi- bilité d'utilisation de cartes D.-card par une organisation "cybercriminelle", est déjà connue dans divers pays. Selon des articles de presse, que nous annexons à l'analyse, des organisations criminelles utiliseraient des logi- ciels malveillants (RANSOMWARE, ou RANÇONGICIEL), qui prennent en otage des données personnelles, pour demander ensuite à leur propriétai- re d'envoyer de l'argent (via Ukash ou D. Sàrl) en échange de la clé

qui leur permettra de les déchiffrer.

Nous avons contacté l'intermédiaire financier qui nous a confirmé que le client a voulu transférer, sans succès (l'intermédiaire financier a bloqué l'opération), presque la totalité des avoirs (>USD 4'400.--) sur sa relation bancaire auprès de la banque C. Un transfert d'argent sur sa relation d'af- faires avait déjà été effectué le 17.03.2012 (USD 296.40).

(…)

A ce jour, nous ne sommes pas en mesure de confirmer les soupçons émis par l'intermédiaire financier quant à une éventuelle origine criminelle

des fonds présents et ayant été crédités avec des recharges D.-card. D. Sàrl mentionne que des transactions liées à la cybercriminalité auraient été effectuées avec l'utilisation des codes PIN perçus par l'extorsion (art. 156 CPS) de la part de vraisemblables organisations criminelles; de telles transactions ont été constatées sur la relation d'affaires de B.

Dans le cas actuel nous ne sommes pas en mesure de prouver que B. ait agi comme partie active d'une organisation liée à la cybercriminalité ou comme agent ayant acheté des recharges D.-card à 60% de leur valeur pour les charger sur son compte auprès de l'intermédiaire financier et les retransférer sur sa relation bancaire auprès de la banque C.

Ce cas présente suffisamment d'indices de détournements frauduleux de fonds (v. courriel de D. Sàrl, la livraison de fausses cartes à l'intermédiai- re, etc.) avec une typologie de criminalité déjà connue dans d'autres pays. Il n'est pas exclu que B. ait blanchi des fonds, en utilisant des recharges D.-card obtenues de façon illicite, en créditant son compte auprès de la société A. SA pour les bonifier ensuite sur sa relation bancaire au Pérou.

L'utilisation de ce système particulier de relations d'affaires électroniques, avec le chargement de recharges "D.-card", obtenues de façon illicite, les transferts internationaux d'"argent électronique" et les observations émi- ses par l'intermédiaire financier, nous incitent à vous transmettre le dos- sier, conformément à l'article 23 al. 4 LBA, afin que vous lui donniez la sui- te que vous jugerez opportune." (act. 1.5).

E. 2.3.2

Les éléments qui précèdent conduisent aux constatations suivantes:

Un citoyen péruvien domicilié au Pérou et n'ayant, en l'état du dossier, au- cun lien avec la Suisse, aurait utilisé un "portefeuille virtuel" – hébergé par un intermédiaire financier sis dans le canton de Fribourg – pour faire transi- ter des fonds d'origine potentiellement criminelle avant de les rapatrier sur un compte bancaire ouvert au Pérou. A ce stade, et sur la (seule) base des éléments au dossier, la question de savoir si les soupçons de blanchiment visant B. portent sur une activité ayant été commise pour une part prépon- dérante en Suisse ou à l'étranger ne peut être tranchée avec précision. Il apparaît néanmoins que les liens personnels – et cela a déjà été relevé – de l'intéressé avec la Suisse semblent inexistants, toutes les démarches que ce dernier a effectuées en rapport avec le portefeuille de la société A. SA l'ayant apparemment été à partir de l'étranger par voie électronique. Les documents d'ouverture dudit portefeuille ont été signés à U. (Pérou) (act. 1.5, p. 2). De telles indications apparaissent de nature à induire que B.

a déployé son activité au Pérou, et que, partant la "part prépondérante" de cette dernière ne l'aurait pas été en Suisse.

Il ressort par ailleurs – et en tout état de cause – de l'ensemble du dossier soumis à la Cour que la présente affaire s'inscrit dans un contexte suprana- tional. Selon les informations recueillies par le MROS auprès de l'intermé- diaire financier, de même que de la société D. Sàrl, certaines des transac- tions opérées par B. pourraient être liées à l'activité d'une organisation de cybercriminalité, laquelle se cacherait derrière les fausses D.-cards no- tamment utilisées par l'intéressé. Les agissements en amont des actes de blanchiment suspectés sur territoire suisses pourraient notamment avoir été commis au moyens de logiciels malveillants (Ransomware ou Rançon- giciel), qui "prennent en otage des données personnelles, pour demander ensuite à leur propriétaire d'envoyer de l'argent (via […] D. Sàrl) en échan- ge de la clé qui leur permettra de les déchiffrer" (v. supra consid. 2.3.1). Ces agissements seraient le fait d'organisations actives à l'étranger dans la cybercriminalité. Un tel contexte peut – et doit – être mis en parallèle avec les cas desdites "attaques d'hameçonnage" (Phishing cases; v. à cet égard le Rapport semestriel 2011/II de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI http://www.news.admin.ch/message/index.html?lang =fr&msg-id=44410) dont la Cour de céans a eu à maintes reprises à traiter ces derniers mois (v. notamment TPF 2011 170). A cette occasion, il a été retenu que de tel- les affaires dans lesquelles il existe des soupçons qu'une partie de l'activité délictueuse soit opérée depuis l'étranger par le biais, entre autres, de logi- ciels malveillants, doivent être confiées à l'autorité la mieux à même de mener à bien de telles investigations, soit en l'occurrence le MPC. En effet, ce dernier dispose des ressources nécessaires en pareils cas, tant au ni- veau des contacts avec l'étranger que des moyens spécifiques en matière de lutte contre la cybercriminalité. Une telle solution s'inscrit au demeurant dans la ligne poursuivie par le "Projet efficacité" à l'origine du renforcement des compétences de la Confédération (v. TPF 2011 170 consid. 2.3). Au vu du contexte dans lequel s'inscrit la présente cause, il n'y a pas lieu de dé- roger à la solution admise pour les cas de Phishing. C'est donc au MPC qu'il reviendra de poursuivre l'enquête qu'il a lui-même ouverte ensuite de la dénonciation du MROS, étant précisé que la distinction opérée dans la jurisprudence relative aux cas de Phishing, entre le "Finanzmanager", d'une part, et les autres participants à l'infraction, d'autre part, n'a pas lieu d'être en l'espèce, toute l'activité délictueuse soupçonnée ayant, en l'état du dossier, été déployée à partir de l'étranger.

- 9 -

E. 3

Il résulte de ce qui précède que la requête du MPC doit être rejetée et que les autorités de poursuite pénale de la Confédération sont déclarées seules compétentes pour poursuivre et juger les infractions concernées par la pré- sente décision.

E. 4

Il n'est pas prélevé de frais (art. 423 al. 1 CPP).

- 10 -