https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-creteil-11eme-chambre-correctionnelle-jugement-du-23-avril-2013/

Jurisprudence : Responsabilité

mercredi 22 mai 2013

Tribunal de Grande instance de Créteil 11ème chambre correctionnelle Jugement du 23 avril 2013

Ministère public / Olivier L.

accès frauduleux - cybercriminalité - données - fraude informatique - maintien frauduleux - mot de passe - sécurité - système de traitement automatisé de données - vol

DISCUSSION

Une convocation à l'audience du 23 avril 2013 a été notifiée à L. Olivier le 11 février 2013 par un agent ou un officier de police judiciaire sur instruction du procureur de la République et avis lui a été donné de son droit de se faire assister d'un avocat.

Conformément à l'article 390-1 du code de procédure pénale, cette convocation vaut citation à personne.

L. Olivier a comparu à l'audience assisté de son conseil ; il y a lieu de statuer contradictoirement à son égard.

Il est prévenu :
– d'avoir à Maisons Alfort, Orléans, dans le département du Val de Marne du 1er août 2012 au 3 septembre 2012, en tout cas sur le territoire national et depuis temps non couvert par la prescription, accédé frauduleusement à tout au partie d'un système de traitements automatisés de données, en l'espèce de l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), faits prévus par art.323-1 al. 1 C.pénal, et réprimés par art.323-1 al 1, art.323-5 C.pénal.
– Pour s'être à Maisons Alfort, Orléans, dans le département du Val de Marne du 1er août 2012 au 3 septembre 2012, en tout cas sur le territoire national et depuis temps non couvert par la prescription, maintenu frauduleusement dans tout ou partie d'un système de traitement automatisé de données, en l'espèce de l'extranet de l'Agence de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), faits prévus par art.323-1 al 1 C.pénal, et réprimés par art, 323-1 al 1, art323-5 C.pénal.
– d'avoir à Maisons Alfort, Orléans, dans le département du Val de Marne du 1er août 2012 au 3 septembre 2012, en tout cas sur le territoire national et depuis temps non couvert par la prescription, frauduleusement soustrait des documents sur l'extranet de l'Agence de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), données téléchargées puis fixées et enregistrées sur plusieurs supports (média center et disque dur), au préjudice de Anses, faits prévus par art.311-1, art.311-3 C.pénal. et réprimés par art.311-3, art.311-14 10, 20, 30, 40, 60 C.pénal.

Sur l'action publique

Le 6 septembre 2012, l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) représentée par Monsieur Nin K., informaticien, déposait plainte auprès des services de police de Maisons-Alfort (94) pour intrusion dans son système informatique et vol de données informatiques.
Il expliquait que le 3 septembre 2012, l'agence avait détecté un accès frauduleux sur son serveur extranet. Cette découverte faisait suite à la découverte par un chef d'unité de I'Anses d'un article relatif aux nano-matériaux mis en ligne sur le site d'information alternatif « reflets.info », article accompagné d'un document "powerpoint" de l'agence et destiné uniquement à un usage interne.

Des premières investigations menées par l'Anses, il ressortait que de nombreux documents avaient été exfiltrés le 27 et le 28 août 2012 vers une adresse IP localisée au Panama. Les personnes ayant récupéré les documents avaient profité d'une faille de sécurité sur le serveur extranet pour y accéder sans avoir à s'identifier et avaient ainsi pu accéder aux documents privés de l'Anses.

La Direction Centrale du Renseignement Intérieur était chargée de la poursuite des investigations, l'Anses étant un opérateur d'Importance Vitale (OIV).

L'audition du responsable technique de l'Anses confirmait les éléments de la plainte, à savoir une erreur de paramétrage du serveur hébergeant l'extranet (ensemble des fichiers accessibles en lecture) qui avait permis le téléchargement depuis une adresse IP d'un VPN localisée au Panama de l'ensemble des fichiers présents sur ce serveur (environ 8Go de données).

Les circonstances de la découverte d'un document interne de l'agence sur le site «Reflets.info» étaient également confirmées. Ce document accompagnait un article consacré à la dangerosité des nano-matériaux et était signé d'une personne utilisant le pseudonyme « ovan M. ».

Les recherches menées sur internet amenaient à découvrir un second article relatif à la légionellose quant à lui signé d'un individu utilisant le surnom «Bluetouff» et était accompagné d'un fichier compressé contenant des documents provenant du serveur extranet de l'Anses.

Ultérieurement, le même «Bluetouff» indiquait être en possession de 7.7 Gigaoctets de documents traitant de santé publique.

L'analyse des journaux de connexions du serveur extranet et du firewall de I'Anses confirmait la primo-analyse réalisée par I'Anses concernant la localisation des adresses IP ayant exfiltré un volume important de fichiers appartenant à l'agence. Si une adresse correspondait à un service VPN suédois pour lesquels il était impossible de connaître le propriétaire, une seconde adresse IP ayant effectué un téléchargement de 8.2 Go de données entre le 27 et le 28 août 2012 était localisée au Panama. Cette adresse IP provenait d'un serveur informatique hébergeant une solution VPN de la société « Toonux.net », fondée et dirigée par Monsieur Olivier L.

Il était en outre également permis d'identifier Monsieur Olivier L. comme étant l'internaute utilisant l'alias « Bluetouff ». Il était placé en garde à vue le 21 novembre 2011.

Lors de ses auditions, Monsieur Olivier L. reconnaissait avoir récupéré via son VPN panaméen l'ensemble des données accessibles sur le serveur extranet de l'Anses. Il déclarait avoir découvert tous ces documents en libre accès après une recherche complexe sur le moteur de recherche Google.

S'il affirmait être arrivé par erreur au cœur de l'extranet de I'Anses, il reconnaissait néanmoins avoir parcouru l'arborescence des répertoires de celui-ci et être remonté jusqu'à la page d'accueil sur laquelle il avait constaté la présence de contrôles d'accès (authentification par identifiant et mot de passe).

Il précisait ne pas avoir diffusé l'archive de 7.7 Gigaoctets qu'il avait généré avec l'ensemble et en avoir seulement fait une extraction de 250 Megaoctets qu'il avait utilisé pour argumenter son article sur la légionellose. Monsieur Olivier L. avouait également avoir communiqué des documents à un autre rédacteur du site «Reflets.info», «Yovan M.», identifié en la personne de Monsieur Pascal H.

Enfin, il acceptait de retirer les fichiers et liens de téléchargement en rapport avec l'Anses sur l'ensemble des serveurs et supports.

Les investigations techniques menées lors de la perquisition au domicile de Monsieur Olivier L. permettaient la récupération de l'archive complète de 7.7 Go.

Le 17 décembre 2012, Monsieur Pascal H., entendu en tant que témoin, confirmait avoir eu accès aux données de I'Anses et avoir utilisé un fichier sur la thématique des « nano-argents » pour illustrer un article. Il reconnaissait en outre avoir rendu public ce fichier sur un site de téléchargement. L'intéressé, sachant que les documents provenaient de la documentation de I'Anses, ignorait en revanche qu'ils avaient été collectés sur un espace privé par Monsieur Olivier L. Il acceptait de retirer le fichier incrimine «Nano Etat des Lieux 2012» de l'espace d'hébergement en ligne utilisé.

Sur l'accès frauduleux et le maintien frauduleux dans un système de traitement automatisé de données

Selon l'article 323-1 du code pénal, le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

L'accès frauduleux à un système de traitement automatisé de données est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation.

En l'espèce, il ressort des déclarations précises et circonstanciées du prévenu que lors de son accès au site extranet de l'Anses, il a remarqué qu'un code utilisateur et un mot de passe pouvaient être demandé pour accéder à certaines données.

Néanmoins, il n'est pas contesté par l'Anses qu'une défaillance technique existait dans le système et que Monsieur Olivier L. a pu récupérer l'ensemble des documents sans aucun procédé de type «hacking».

Par ailleurs, Monsieur Olivier L. a pu justifier l'utilisation du VPN panaméen, celui-ci lui servant dans le cadre de sa société Toonux.net.

Compte tenu de l'ensemble de ces éléments, même s'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection, le maître du système, l'Anses, en raison de la défaillance technique, n'a pas manifesté clairement l'intention de restreindre l'accès aux données récupérées par Monsieur Olivier L. aux seules personnes autorisées.

Monsieur Olivier L. a pu donc légitimement penser que certaines données sur le site nécessitaient un code d'accès et un mot de passe mais que les données informatiques qu'il a récupérées étaient en libre accès et qu'il pouvait parfaitement se maintenir dans le système.

En conséquence, il convient de relaxer Monsieur Olivier L. des chefs d'accès frauduleux et maintien frauduleux dans un système de traitement automatisé des données.

Sur le vol des documents téléchargés et enregistrés sur plusieurs supports

Selon l'article 311-1 du code pénal, le vol est la soustraction frauduleuse de la chose d'autrui.

En l'espèce, en l'absence de toute soustraction matérielle de documents appartenant à l'Anses, le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques de l'Anses qui n'en a jamais été dépossédée, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose.

En tout état de cause, Monsieur Olivier L. a pu légitimement penser que ces documents étaient librement téléchargeables puisque non protégés par un quelconque système. Il n'y a pas eu de sa part une volonté d'appropriation frauduleuse de ces fichiers informatiques et donc il n'y a pas d'élément intentionnel de l'infraction.

DÉCISION

Le tribunal, statuant publiquement, en premier ressort et contradictoirement à l'égard de L. Olivier,

. Relaxe L. Olivier des fins de la poursuite.

Le tribunal : M. Jean-Louis Peries, Mme Marie Hiribarren et M. Jean-Loup Chanal (assesseurs)

Avocat : Me Olivier Iteanu