Accès frauduleux à un système de traitement automatisé de données : chacun doit sécuriser son système informatique !

[INFORMATIQUE]
TGI Créteil, 11ème Ch. Corr., 23 avril 2013, Ministère Public / Olivier L.
Cass. Crim., 10 avril 2013, Robert X. / Conseil constitutionnel

Sécuriser son système informatique n'est pas simplement un acte de bon sens, c'est également une action qui peut avoir des conséquences juridiques.

En l'espèce, l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) avait détecté une intrusion dans son système informatique suite à la découverte sur internet de la mise en ligne d'un article accompagné d'une présentation destinée à un usage interne.

L'enquête qui avait alors été diligentée avait permis d'identifier la personne qui s'était procurée ce document confidentiel. Sans nier avoir récupéré l'ensemble des données accessibles sur le serveur extranet de l'agence, le prévenu indiquait néanmoins y être arrivé par erreur et avoir alors parcouru l'arborescence des répertoires dudit serveur. En outre, il précisait n'avoir diffusé qu'une très faible partie des archives auxquelles il avait eu accès.

En premier lieu, le Tribunal a rappelé les termes de l'article 323-1 du code pénal précisant que l'infraction d'accès frauduleux à un système de traitement automatisé de données est constituée « *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.* ».

Or, en l'espèce, il était démontré – et non contesté – que le système informatique litigieux comportait une défaillance technique qui avait permis au prévenu d'obtenir l'ensemble des documents litigieux « *sans aucun procédé de type « hacking »* », alors que l'accès à certaines données nécessitait un code utilisateur et un mot de passe.

Le Tribunal a ainsi considéré que «*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*», le prévenu pouvant alors légitimement penser que seules les données protégées par des identifiants n'étaient pas libres d'accès.

Dès lors, si le Tribunal a précisé que l'infraction ne nécessite pas pour être constituée qu'un système de protection soit nécessairement mis en place, il a conclu, dans le cadre d'une analyse *in concreto*, que l'agence n'avait pas clairement démontré sa volonté que l'accès à ses données soit restreint.

Le Tribunal a également rejeté le chef d'accusation de vol, considérant qu'il n'y avait eu aucune soustraction matérielle en l'espèce.

Le prévenu a donc été relaxé.

Dans un souci d'exhaustivité, précisons que par un arrêt du 10 avril 2013, la Cour de cassation a statué sur une demande de renvoi au Conseil constitutionnel d'une question prioritaire de constitutionnalité relative à l'article 323-3 du code pénal relatif à l'introduction et la modification frauduleuses de données dans un système de traitement automatisé.

La Cour de cassation a estimé que la question prioritaire de constitutionalité posée « *ne présente pas (…) un caractère sérieux dès lors que les termes de l'article 323-3 du code pénal sont suffisamment clairs et précis pour que son interprétation et sa sanction, qui entrent dans l'office du juge pénal, puissent se faire sans risque d'arbitraire.* ». La Cour a donc refusé de renvoyer la question prioritaire de constitutionalité au Conseil constitutionnel.

Olivier HAYAT

13, rue Alphonse de Neuville 75017 Paris Tél 33 1 43 18 55 00 Fax 33 1 43 18 55 55
SELARL au capital de 196 612 € Toque n° L237 420 483 844 RCS Paris