Le défaut de sécurisation d'un extranet face à l'accès et au maintien frauduleux dans un système de traitement automatisé de données

[INTERNET]
Cass. crim., 20 mai 2015

La protection des données des entreprises et organismes gouvernementaux est un sujet particulièrement d'actualité.

Un journaliste animant un site internet d'information avait accédé à de nombreux documents confidentiels de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Ces données étaient stockées sur le site extranet de l'agence, dont l'accès nécessitait une identification préalable. En raison d'un défaut de configuration des serveurs, des liens vers cet espace avait été indexés par un moteur de recherche grand public, qui devenait librement accessible. Le journaliste avait pu, par une recherche « complexe » sur ce moteur, procéder au téléchargement des documents.

Après la publication sur son site d'une partie de cette documentation non destinée au public, le prévenu était mis en garde à vue puis poursuivi notamment pour « *accès et maintien frauduleux dans un système de traitement automatisé de données* », qualification pénale délictuelle prévue à l'article 323-1 du Code pénal. Le journaliste reconnaissait les faits au cours de cette garde à vue, et admettait qu'au cours de sa navigation sur le site extranet, il était arrivé sur une page d'accueil, protégée par un contrôle d'accès, mais avait néanmoins poursuivi sa navigation.

Relaxé en première instance, il est néanmoins condamné en appel pour maintien frauduleux dans un système de traitement automatisé de données, et vol de données informatiques. La Chambre criminelle de la Cour de cassation confirme le 20 mai 2015 cet arrêt. Elle énonce en effet que le prévenu *« s'est maintenu dans un système de traitement automatisé après avoir découvert que celui-ci était protégé et a soustrait des données qu'il a utilisées sans le consentement de leur propriétaire »*.

En raison du défaut de sécurisation, la Cour d'appel avait abandonné la qualification d'accès frauduleux. Le juge pénal retient cependant la qualification de maintien frauduleux, considérant que le prévenu « *avait conscience de son maintien irrégulier dans le système de traitement automatisé de données visité* » et avait caractérisé l'intention du délit.

Il est intéressant de relever que les qualifications d'accès et de maintien frauduleux dans un traitement automatisé de données sont indépendantes, et que l'absence de caractère frauduleux de l'accès ne présume pas de l'absence de caractère frauduleux du maintien dans le système. L'on retiendra que le défaut de sécurisation permettant un libre accès ne permettait pas de qualifier le caractère frauduleux de cet accès, ce que confirme la Cour.

En revanche, concernant le caractère frauduleux du maintien dans le système, le caractère intentionnel est à notre sens déterminant en l'espèce : en admettant avoir eu conscience que l'accès nécessitait en principe une identification, il validait l'intentionnalité et donc le caractère frauduleux.

Enfin, la qualification du téléchargement comme vol de données, déjà reconnue par la jurisprudence, n'est pas remise en cause par la Cour de cassation. Elle confirme l'appréciation de la Cour d'appel selon laquelle la réalisation de « *copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire* » constitue un vol au sens de l'article 311-1 du Code pénal.

Loïc FOUQUET

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