La légalisation du hacking d'enquête ou de la perquisition électronique par la loi du 14 mars 2011

publié le **20/07/2011**, vu **5365 fois**, Auteur : Anthony BEM

La communication numérique a donné naissance à de nouveaux types de contentieux, d'infractions pénales et de méthode d'investigation policière. Les nouvelles technologies contraignent les enquêteurs à rechercher des éléments de preuves sur les réseaux de communication numérique, l'internet ou sur des équipements nomades. Le législateur a tenu compte de la nécessité pour les forces de l'ordre d'enquêter aussi sur le web et les réseaux sociaux. Ce faisant, la loi n° 2011-267, du 14 mars 2011, dite d'orientation et de programmation pour la performance de la sécurité intérieure, dite LOPSI 2, a légalisé le hacking au détour des dispositions de l'article 706-102-1 du Code de Procédure Pénale.

Ce nouvel article inséré dans le Code de Procédure Pénale, au chapitre intitulé *renforcement de la lutte contre la criminalité et de l'efficacité des moyens de répression,* dispose que :

> *« Lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée* ***les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères.*** *Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction ».*

Ainsi, les enquêteurs pourront pénétrer, à distance, au sein des ordinateurs pour enregistrer, conserver et transmettre des données informatiques.

Elle constitue donc une exception à l'article 226-3 du code pénal qui dispose que :

> *« Est punie des mêmes peines la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'Etat, d'appareils ou de dispositifs techniques conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue par l'article 706-102-1 du code de procédure pénale et figurant sur une liste dressée dans des conditions fixées*

par ce même décret ».

Par le passé la chambre criminelle de la Cour de cassation avait déjà eu l'occasion de juger que le dispositif de captation et d'enregistrement de conversations tenues au parloir d'une maison d'arrêt, ordonnées par le juge d'instruction pour une durée limitée et placées en permanence sous son autorité et son contrôle, a été justifié par la nécessité de rechercher la manifestation de la vérité, relativement à des infractions portant gravement atteinte à l'ordre public, à savoir recel de blanchiment aggravé de produits provenant du trafic de stupéfiants (Cass. Crim, 1er mars 2006, N° de pourvoi: 05-87251 ; Cass. Crim., 9 juillet 2008, N° de pourvoi: 08-82091)

Le juge d'instruction peut donc désormais autoriser un *« dispositif technique ayant pour objet, sans le consentement des intéressés , d'accéder en tous lieux, à des données informatiques »* .

A cet égard, l'article 32 de la Convention Internationale de Budapest sur la cybercriminalité, intitulé "Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public", qui a été ratifiée par la France en 2006, prévoit expréssement la possibilité d'un accès transfrontière à des données stockées conditionné par un consentement « légal et volontaire » :

« Une Partie peut, sans l'autorisation d'une autre Partie :

- a) accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

- b) accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique ».

La loi du 14 mars 2011 instaure donc une véritable perquisition électronique sans prévoir les modalités précises de ce type de pouvoir d'investigation policière.

Un amendement a donc été déposé le 8 février 2010 par les députés Mesdames Berthelot , Girardin, Jeanny Marc , Orliac , Pinel , Robin-Rodrigo et Messieurs Charasse , Giraud, Likuvalu et Giacobbi tendant à ce qu'après le mot « technique » soit inséré le mot « proportionné ».

Ainsi, cet amendement visait à assurer que les mesures techniques d'« écoute » sur les communications électroniques soient strictement proportionnées à leur finalité, notamment dans leurs atteintes aux droits et libertés des personnes qui en font l'objet.

Malgré que cet amendement n'ait pas donné lieu à une modification du texte de loi, le contrôle de cette proportionnalité appartient au juge d'instruction.

Pour l'heure, il existe peu de jurisprudence relative à l'application de cette nouvelle disposition et même de commentaires ou de débats autour de cette nouvelle mesure d'investigation policière totalement absente des autres régimes juridiques nationaux.

En tout état de cause, il convient de relever que l'utilisation judiciaire des nouvelles technologies se développe rapidement.

L'iPhone d'Apple permet déjà à la police américaine d'identifier les délinquants.

En effet, la société américaine BI2 Technologies a conçu et commercialise un lecteur d'empreintes

digitales ou d'iris qui se dénomme MORIS (Mobile Offender Recognition and Identification System) et qui se connecte à un iPhone pour identifier une personne grâce à l'application photo de l'iPhone.

Ainsi, lorsqu'un policier identifie un individu ayant commis une infraction, il prend soit une photographie, l'empreinte digitale ou l'iris d'une personne afin de la comparer à la base de données des personnes ayant déjà commis un délit et le cas échéant agir en conséquence.

Cette nouvelle application est sur le point d'être développée sur les appareils dits Android, les Windows Phone.

"*Big Brother is Watching you* [illegible] Orwell)

Je suis à votre disposition pour toute information ou action.

PS : Pour une recherche facile et rapide des articles rédigés sur ces thèmes, vous pouvez taper vos "mots clés" dans la barre de recherche du blog en haut à droite, au dessus de la photographie.

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
Tel : 01 40 26 25 01

Email : abem@cabinetbem.com

www.cabinetbem.com