Infractions et numérique – Quelles réponses du droit pénal ?

Elisa BARON, Maître de conférences en droit privé, Université de Bordeaux

Le développement du numérique va de pair avec celui des infractions commises grâce à cet outil ou à son égard. En tant que moyen de communication, le numérique permet de développer de façon exponentielle les activités illicites « traditionnelles » comme le trafic de stupéfiants ou encore l'escroquerie, et d'accroître le nombre de leurs victimes. Par ailleurs, la naissance et le développement du numérique ont nécessairement entraîné la naissance de comportements répréhensibles propres à la matière, tels que le piratage informatique. Comment le droit pénal appréhende-t-il ces phénomènes ? Dispose-t-il d'armes efficaces ? Autrement dit, a-t-il su s'adapter à la « révolution numérique » ?
Ces différents comportement sont autant de défis pour le droit pénal, défis qui touchent aussi bien à l'incrimination des comportements répréhensibles en la matière, qu'à la mise en œuvre de la répression pénale.

S'agissant en premier lieu du principe de la répression, le droit pénal utilise d'abord les infractions classiques, de droit commun, pour sanctionner nombre de comportements. Par exemple, les vols de données informatiques sont appréhendés par l'intermédiaire du vol de l'article 311-1 du code pénal, et les messages outrageants ou injurieux postés sur les réseaux sociaux peuvent être sanctionnés à travers la diffamation et l'injure prévus par la loi de 1881. Plus généralement, l'escroquerie, l'abus de confiance, l'usurpation d'identité, les falsifications ou les atteintes à la vie privée sont fréquemment employés pour réprimer des comportements commis informatiquement. Cette utilisation des incriminations de droit commun soulève des questions importantes. Est-elle efficace ou laisse-t-elle place à des vides juridiques privant de sanction des comportements pourtant choquants ? Ne conduit-elle pas à adapter ces incriminations, quitte à les dévoyer et mettre ainsi à mal le principe de légalité criminelle ? De plus, ces textes sont loin d'épuiser tous les comportements répréhensibles commis informatiquement.

C'est pourquoi ensuite, le droit pénal a prévu des infractions spécifiques pour lutter contre les comportements propres au numérique. Ainsi, il appréhende le piratage informatique à travers l'incrimination des atteintes aux systèmes de traitement informatisé de données (STAD) aux articles 323-1 et suivants du Code pénal. Y sont sanctionnés par exemple, l'introduction et le maintien dans ces STAD. Dans le même ordre d'idées, le Code de la

propriété intellectuelle sanctionne la négligence caractérisée consistant notamment à ne pas avoir mis en place un moyen de sécurisation de son accès internet[1], afin de protéger la propriété littéraire et artistique. Là encore, ces textes posent la question de leur efficacité et de leur complétude avec les infractions de droit commun précédemment évoquées.

En second lieu, au-delà du principe même de la répression, reste à s'interroger sur sa mise en œuvre. En effet, même s'il était acquis que ce dispositif permet d'appréhender tous les comportements envisageables commis par la voie informatique, l'anonymat rendu possible grâce à internet fait véritablement s'interroger sur les outils dont dispose le droit pénal pour débusquer les coupables et mettre en œuvre la répression. A cet égard, le Darkweb est révélateur. Le Darkweb, également appelé Deepweb, est une partie du net non référencée sur les moteurs de recherche traditionnels tels que Google ou Firefox, à laquelle tout un chacun n'a généralement pas accès. Cet internet « masqué » permet de garantir l'anonymat de ses utilisateurs et se révèle ainsi être une véritable plateforme pour les activités illégales. Pédopornographie, trafic de drogue, trafic d'armes, trafic d'êtres humains ou encore blanchiment y sont légion. Les cyberperquisitions mises en place par la loi LOPPSI II[2] sont-elles une réponse suffisante de la législation française ? Par ailleurs, ces activités posent nécessairement la question de l'application de la loi pénale dans l'espace et plus généralement de la coopération internationale en la matière.

Voici ainsi rapidement quelques-unes des questions qui feront l'objet de notre étude.

[1] Art. R. 335-5

[2] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, qui crée un article 706-102-1 dans le Code de procédure pénale rédigé de la sorte :
« 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. ». L'article a été plusieurs fois modifié depuis.