Pour nous contacter
Equipe IP/IT & Data Protection
ebarbry@racine.eu |
(+33) 6.13.28.91.28

La Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur est passez plutôt inaperçue dans les actualités relatives au numérique. Toutefois, malgré son intitulé peu évocateur, ses conséquences en matière de répression de la cybercriminalité sont importantes.

Tout d'abord, un peu de contexte :

L'étude d'impact[1] associée estime qu'entre 2016 et 2020, pas moins de 1580, voire 1870 procédures en lien avec des attaques par rançongiciels à l'encontre d'entreprises et d'institutions ont été enregistrées par les forces de police et de gendarmerie. Ces chiffres ne concernent que les seules attaques par rançongiciels, et plus encore, ils ne concernent que les seules procédures enregistrées, ces dernières étant souvent minoritaires au regard de la quantité d'attaques véritablement orchestrées.

Les constations du rapport annexé[2] au projet de loi sont également très parlantes :

- Augmentation des faits de cyberdélinquance de 10% à 20% chaque année ;
- En 2019, 50% des utilisateurs de 15 ans au moins ont été témoins de faits de cybercriminalité, en particulier via des redirections vers des sites frauduleux ;
- En 2020, une entreprise sur cinq affirmait avoir subi (au moins) une attaque par rançongiciel pendant l'année ;
- 58% des cyberattaques ont impacté directement l'économie des acteurs concernés, cet impact atteignant la production même de ces acteurs dans 27% des cas.

Le législateur s'est donc emparé du problème et a procédé à de nombreuses évolutions législatives de lutte contre la cybercriminalité.

Tel est le cas avec cette loi n° 2023-22 du 24 janvier 2023 (la « Loi »).

En premier lieu, la Loi augmente le plafond des sanctions relatives aux atteintes aux systèmes de traitements automatisé de données (Articles 323-1 et suivants du Code pénal).

L'article 323-1 du Code pénal sanctionne le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, ainsi que la suppression, la

[1]https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/ei_art_39_2022/ei_iomd2223411l_cm_7.09.2022.pdf
[2]https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/actualite-legislative/2022/pjl_iomd2223411l_rapport-annexe_cm_7.09.2022.pdf

modification de données contenues dans le système, ou bien encore une altération du fonctionnement de ce dernier.

Les modifications apportées par la Loi sont les suivantes :

Thème	Version antérieure	Version nouvelle
Accès et maintien frauduleux dans un SI	2 ans d'emprisonnement 60 000 euros	3 ans d'emprisonnement 100 000 euros
Suppression, modification ou altération du SI	3 ans d'emprisonnement 100 000 euros	5 ans d'emprisonnement 150 000 euros
S'agissant d'un SI mis en œuvre par l'Etat (pour les mêmes infractions : accès, maintien, suppression, modification ou altération du SI)	5 ans d'emprisonnement 150 000 euros	7 ans d'emprisonnement 300 000 euros

Le législateur semble également avoir pris en compte l'impact certain de la cybercriminalité, et en particulier des rançongiciels, sur le système de santé : en 2020, pas moins de 27 attaques de grande envergure ont en effet impacté les établissements de santé, mettant par conséquent la vie de nombreux patients en jeu. Certains chiffrent évoquent même au moins une attaque hebdomadaire à l'encontre des hôpitaux.[3]

A cet égard, la Loi créé un nouvel article 323-4-2 du Code pénal, portant à 10 ans d'emprisonnement et 300 000 euros d'amende les sanctions, si les atteintes aux systèmes d'information ont pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes.

Au-delà des seules atteintes aux systèmes d'information, les structures étroitement liées au « Darknet » et au « Darkweb » semblent également être dans le viseur du législateur.

Le nouvel article 323-3-2 du Code Pénal initie ainsi la pénalisation des opérateurs de plateforme en ligne qui garantissent l'anonymat à leurs utilisateurs en restreignant leurs accès aux seuls utilisateurs utilisant des techniques d'anonymisation des connexions, en dépit des obligations de conservation des métadonnées et de suppression des contenus illicites prévues par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Article 6). La plateforme doit également leur « permettre sciemment » de céder des produits, contenus, ou services, dont la cession, l'offre, l'acquisition ou la détention sont manifestement illicites. Cette infraction est sanctionnée par 5 ans d'emprisonnement et une amende de 150 000 euros.

[3] https://esante.gouv.fr/sites/default/files/2022-01/DP-CYBERSECU-MONTE-201625-WEB.pdf

En outre, ces sanctions s'appliquent dorénavant également au fait de proposer, par l'intermédiaire de ces plateformes ou au soutien des transactions qu'elles permettent, des prestations d'intermédiation ou de séquestre ayant pour seul ou principal objet de mettre en œuvre, dissimuler ou faciliter ces opérations. Si les tentatives de commission de ces infractions sont sanctionnées des mêmes peines, elles sont portées à 10 ans d'emprisonnement et à 500 000 euros d'amende en cas de commission en bande organisée.

Les évolutions en matière de lutte contre la cybercriminalité ne s'arrêteront bien sûr pas à ces quelques évolutions. Le rapport annexé prévoit notamment la mise en place d'un équivalent numérique du numéro de téléphone associé aux forces de l'ordre (le 17) afin de permettre aux citoyens de signaler une infraction cyber et d'entrer en contact avec un agent spécialisé dans les plus brefs délais.

Les entreprises quant à elles restent vivement incitées à poursuivre leurs efforts en matière de sécurisation de leurs systèmes d'informations et à se faire accompagner des meilleurs professionnels en cas de survenance d'une cyberattaque.

Et dans l'attente de la mise en place d'un éventuel numéro de téléphone adapté, elles peuvent naturellement se tourner vers l'équipe IP/IT & Data Protection de Racine !

Eric Barbry
Avocat associé
ebarbry@racine.eu

Olivier Quelin
Juriste
oquelin@racine.eu