La LOPMI et la transformation numérique des moyens de la sécurité intérieure

Bertrand Warusfel

2099

La LOPMI et la transformation numérique des moyens de la sécurité intérieure

Bertrand Warusfel,
professeur à l'université Paris 8,
vice-président de l'Association française de droit de la sécurité et de la défense (AFDSD),
avocat au barreau de Paris

La loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur annonce fièrement qu'elle a notamment pour objectif de « *remettre le numérique au cœur de l'activité du ministère de l'intérieur* ». On pourrait gloser sur cette formule qui sous-entend que le numérique aurait été un temps central pour le ministère de l'Intérieur puis qu'elle aurait cessé de l'être. On prendra pourtant cette affirmation au sérieux dès lors que – à défaut d'annonces majeures en la matière – la nouvelle loi de programmation consacre plusieurs articles de sa partie normative à envisager soit le renforcement des moyens numériques de l'État (1), soit à incriminer de nouvelles formes de cybercriminalité (2), soit au moins à renforcer et compléter les dispositions répressives préexistantes en la matière (3).

1. Le renforcement des moyens numériques de lutte contre la délinquance et la criminalité

A. - Annonce d'une nouvelle agence du numérique

1 - S'agissant des moyens confiés aux policiers et aux gendarmes, la LOPMI commence par une annonce qu'elle présente comme importante, à savoir celle de la création d'une « *agence du numérique des forces de sécurité intérieure* » qui devrait aider à ce que « *le policier et le gendarme de demain seront " augmentés " grâce à des outils numériques mobiles tant pour la procédure pénale que pour leurs missions de sécurité* ».

Mais première déception, aucune disposition normative concernant cette entité ne figure dans le texte, dès lors que la définition des missions, des moyens et du rattachement administratif de cette nouvelle « *agence* » relèveront certainement du pouvoir réglementaire. Tout au plus, apprend-on dans les travaux parlementaires que les rapporteurs sénatoriaux ont appris que cette « *agence* » serait « *construite à partir d'un renforcement du STSI* » (l'actuel service des technologies et des systèmes d'information de la sécurité intérieure). Elle devrait également développer des *outils numériques au service du terrain et de l'opérationnel.*

B. - La création d'un opérateur public des communications électroniques des services de secours et de sécurité

2 - Toujours s'agissant du renforcement des capacités numériques du ministère de l'Intérieur, l'article 11 de la LOPMI organise administrativement et juridiquement le futur « *réseau de communications électroniques des services de secours et de sécurité* », c'est-à-dire ce que l'on appelle souvent le « *réseau radio du futur* » (RRF). Ce réseau est défini par la loi comme « *un réseau dédié aux services publics mutualisés de communication mobile critique à très haut débit pour les seuls besoins de sécurité et de secours, de protection des populations et de gestion des crises et des catastrophes* ».

Mais ici la loi n'intervient pas tant pour définir le périmètre de ce nouveau réseau numérique à construire dans les années à venir. Elle est nécessaire tout d'abord pour prévoir qu'il sera mis en œuvre non par un opérateur de communications électroniques privé sélectionné à la suite de l'attribution d'un contrat de concession, mais plus directement par un « *établissement public chargé d'assurer le service public d'exploitation du réseau de communications électroniques des services de secours et de sécurité* » *(CPCE, art. 15 ter nouveau)*. Cet opérateur, qui va être dénommé « *l'Agence des communications mobiles opérationnelles de sécurité et de secours* » (ACMOSS) aura notamment pour mission d'offrir à une vaste communauté (de plus de 350 000 utilisateurs des services de sécurité et de secours) la possibilité d'échanger des communications mobiles critiques à très haut débit (c.-à-d. des échanges prioritaires pour faire face aux exigences de sécurité ou de gestion de crises ou de catastrophes).

Mais la loi vient aussi compléter ce dispositif en créant un nouvel article L. 34-16 CPCE qui va imposer de nouvelles contraintes de service public aux opérateurs privés de communication électroniques, lesquels vont devoir garantir la continuité et la permanence des communications mobiles critiques à très haut débit. En effet, en matière de télécommunications, c'est l'interconnexion des réseaux qui fait la communication. Le nouvel article va donc imposer à ces opérateurs des réseaux grand public de faire droit aux « *demandes d'itinérance, sur leurs réseaux, de l'opérateur du réseau de communications électroniques des services de secours et de sécurité* ». Une convention conclue entre eux et sous le contrôle de l'ARCEP organisera les conditions techniques et financières de cet accord d'itinérance qui prévoira également qu'en « *cas de congestion* » (not. à la suite d'un incident ou un mouvement de foule), les opérateurs de réseaux doivent garantir l'acheminement prioritaire des communications critiques.

2. La lutte contre des nouvelles formes numériques de criminalité

3 - La LOPMI ne se contente pas de renforcer les moyens techniques du ministère de l'Intérieur et des forces de sécurité ou de secours. Elle entend également prendre en compte les dimensions technologiques de la délinquance. Deux dispositions de la LOPMI visent donc particulièrement à renforcer la protection contre ces nouvelles formes de criminalité numérique.

A. - Responsabilité pénale de l'opérateur de plateforme qui tolère un commerce illicite

4 - La responsabilisation des intermédiaires du commerce électronique, et plus particulièrement des plateformes qui permettent aux internautes d'échanger entre eux contenus ou produits, est l'une des thématiques récurrentes du droit contemporain du numérique (à tel point que le nouveau règlement DSA comporte des dispositions visant notamment à pousser les grands opérateurs de services numériques à mieux coopérer à la lutte contre les contenus illicites en ligne).

Dans cette matière, l'article 4 de la LOPMI vient de créer un nouvel article 323-3-2 du Code pénal qui punit, de 5 ans d'emprisonnement et de 150 000 € d'amendes, la plateforme qui permet « *sciemment la cession de produits, de contenus ou de services dont la cession, l'offre, l'acquisition ou la détention sont manifestement illicites* » alors même que cet opérateur favorise la connexion anonyme à son service ou ne conserve pas les éléments d'authentification que l'article 6 de la LCEN impose à tout intermédiaire de recueillir en vue de pouvoir ultérieurement répondre à d'éventuelles réquisitions. Une telle infraction vise donc clairement à mettre la pression le commerçant en ligne (et si nécessaire à pouvoir obtenir sa condamnation et la fermeture des sites de commerce et d'échanges en ligne qui tolère – voire encourage – la commission de différentes activités illicites dont le butin est ensuite proposée sur le web (ou sur le *darknet*).Elle est complétée par un deuxième délit qui vise précisément le fait d'administrer une telle plateforme lorsque celle-ci a pour but unique ou principal de favoriser un tel commerce illicite en ligne. Ce délit est même considéré désormais comme constituant une forme de délinquance organisée *(CPP, art. 706-73-1 mod.)*.

B. - L'encadrement de l'assurance contre les actes de cyberdélinquance

5 - L'article 5 de la LOPMI vise également à appréhender (de manière plus indirecte) de nouvelles formes de cybercriminalité. Ici, il s'agit des attaques par rançongiciel avec demande de rançon. Face à de telles situations, de nombreuses entreprises victimes hésitent à porter plainte et préfèrent parfois payer la rançon demandée, au risque de ne pas permettre l'enquête judiciaire et la poursuite des délinquants concernés.

Pour dissuader ces attitudes qui font le jeu des cyberdélinquants, la LOPMI créé dans le Code des assurances un nouvel article L. 12-10-1 qui réserve la prise en charge par les compagnies d'assurances du préjudice économique causé par une attaque sur un système automatisé de traitement de l'information, au seul cas où aura été effectué le « *dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime* ». Mais assez logiquement cette contrainte ne s'applique qu'aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle.

3. Renforcer et compléter les dispositions répressives préexistantes

A. - Le renforcement des dispositions réprimant les actes de fraude informatique

6 - Depuis l'adoption de la loi Godfrain en janvier 1988, les dispositions aujourd'hui codifiées aux articles 323-1 à 323-8 du Code pénal constituent le cœur de la riposte pénale contre les différentes formes de cyberattaques.

La LOPMI ne remet pas en cause ce dispositif. Bien au contraire, elle le renforce même si – ce faisant – elle peut sembler nuire à la progressivité de certaines peines. Ainsi l'infraction de base, à savoir celle de pénétration non autorisée dans un système de traitement automatisé de données (STAD) voit ses peines fortement augmentées : 2 années supplémentaires pour les peines de prison et une augmentation des amendes significatives (allant jusqu'au doublement de 150 000 € à 300 000 € lorsque les serveurs de l'État sont attaqués).

De ce fait, les peines prévues pour sanctionner les seules atteintes à l'intégrité *(C. pén., art. 323-2 à 323-3)* sont désormais du même niveau que celles fixées aux alinéas 2 et 3 de l'article 323-1 en cas de circonstances aggravantes.

Plus nettement encore, l'article 7 de la LOPMI punit désormais des peines les plus lourdes, la commission de ces différentes infractions en bande organisée et sans autre condition, alors que jusqu'alors, la peine de 10 années d'emprisonnement était réservée aux attaques effectuées en bande organisée à l'encontre des seuls serveurs de l'État *(C. pén., art. 323-4-1, mod.)*.

Enfin, une nouvelle infraction cybercriminelle est créée par l'article 8 de la LOPMI : l'atteinte à un système de données « *qui a 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* » *(C. pén., art. 323-4-2 nouveau)*. Il est vrai que la numérisation croissante d'un nombre toujours croissant d'activités de la vie quotidienne rend celles-ci vulnérables aux effets directs ou indirects d'une attaque cyber sur un système physique dont le dysfonctionnement pourrait notamment blesser une victime.

B. - Les nouvelles possibilités de saisie des actifs numériques

7 - La numérisation concerne non seulement le *modus operandi* des infractions commises mais également la manière dont les délinquants vont capitaliser le produit de leurs délits. Dès lors, la riposte judiciaire doit s'adapter pour continuer à toucher les délinquants « *au portefeuille* », pour reprendre la formule consacrée.

C'est ainsi que l'article 3 de la LOPMI modifie l'article 706-154 du Code de procédure pénale afin de prévoir qu'à côté des saisies en

numéraire, les officiers de police judiciaire spécialement mandatés pour cela, puissent saisir toute somme d'argent, y compris auprès d'un « *établissement habilité par la loi à tenir des comptes de dépôts ou d'actifs numériques mentionnés à l'article L. 54 – 10-1 du code monétaire et financier* ».

Avec cette disposition, la répression pénale intègre donc les nouvelles formes de valeurs numériques, comme les crypto-monnaie, ce qui est bien approprié alors que l'on sait que ces nouvelles formes de placement sont assez prisées par les délinquants du fait de leur relatif anonymat et de leur portabilité.

On signalera enfin que l'article 29 de la LOPMI oblige désormais le ministère de l'Intérieur à publier annuellement deux rapports publics sur sa lutte contre la cybercriminalité, l'un concernant la protection des collectivités territoriales et l'autre celles des entreprises.

Même si la LOPMI du 24 janvier 2023 ne comporte donc pas beaucoup de nouveaux instruments numériques de sécurité, elle manifeste cependant assez clairement la volonté du ministère de l'Intérieur de prendre en compte les effets de la numérisation sur à la fois la nature des infractions et les moyens d'y faire face. Reste, comme l'indique bien le rapport accompagnant la LOPMI, à ne pas sous-estimer le fait que « *l'utilisation des nouvelles technologies dans les domaines de la sécurité ne peut faire l'économie d'une acceptation de la société civile* ». Ce volet politique et sociologique est peu présent dans le texte. Il sera pourtant un élément important du succès (ou de l'échec) de la mise en œuvre de ses nouvelles dispositions. ■