SANCTIONS INTERNATIONALES, LE GEL DES AVOIRS EUROPÉENS DES CYBERATTAQUANTS

Sandra BIRTEL
Rédactrice en chef
CEO de BLL Consulting
Managing Partner de RegMate

Le gel des avoirs est une sanction prise à l'égard d'une personne physique ou d'une personne morale qui vise à bloquer la disposition et à geler ses ressources financières. Sont ainsi concernés les actifs financiers et les avantages économiques de toutes natures ainsi que les avoirs de toutes natures, immobiliers ou mobiliers, corporels ou incorporels, bref, tous les facteurs de richesse.

Après l'adoption d'une de ces sanctions, il est strictement interdit, en vertu d'une obligation de résultat, à toute personne ou entreprise détenant des fonds, de les mettre à disposition d'une personne sanctionnée.

Cela ne concerne pas uniquement les services financiers, mais **toute personne** détenant des fonds comme l'a précisé la toute récente ordonnance n° 2020-1342 du 4 novembre 2020 en France. Il est à noter que cette précision existait déjà depuis bien longtemps dans la loi luxembourgeoise en ces termes : « Les interdictions et mesures restrictives s'imposent aux Luxembourgeois, personnes physiques et morales, ainsi qu'à toutes autres personnes physiques et morales qui opèrent sur ou à partir du territoire luxembourgeois. »[1]

Adopté généralement dans le cadre de la lutte contre le financement du terrorisme, le cœur de cette sanction se trouve dans la Résolution onusienne 1373 de 2001 qui oblige chaque État membre à se doter d'un système de gel des avoirs. Obligation reprise d'ailleurs dans les recommandations du GAFI, plus précisément dans les recommandations 5, 6 et 7, cette sanction occupe une bonne partie du quotidien des *compliance officers*.

Ce qu'il y a d'étonnant est que le gel des avoirs est aujourd'hui un nouveau vecteur du croisement des chemins *Cyber & Compliance*…

Cette sanction, lourde de sens, lourde de conséquences, n'est plus une menace pour les seuls terroristes, du moins ceux qui nous viennent directement à l'esprit. En effet, aujourd'hui, le gel est une menace pour d'autres criminels terrorisant de plus en plus civils et entreprises… j'ai nommé les cyberattaquants.

En effet est apparu en toute discrétion un règlement européen, le règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres. Ce règlement fait lui-même référence à une décision (PESC) 2019/797 « pour des mesures restrictives ciblées visant à dissuader et contrer les cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres. Les personnes, entités et organismes faisant l'objet des mesures restrictives sont inscrits sur la liste qui figure à l'annexe de ladite décision. »

Ainsi donc, vous l'aurez compris, dans le but de dissuader les prochaines cyberattaques majeures, il a été décidé au niveau européen de prendre des mesures restrictives de gel des avoirs à l'encontre de cyberattaquants. Cette décision, outre sa symbolique, fixe la définition d'une cyberattaque et des facteurs qui la rendent passible de ces sanctions.

Ainsi, selon l'article 1er de cette décision PESC telle que modifiée, « la présente décision s'applique aux cyberattaques ayant des effets importants, y compris les tentatives de cyberattaques ayant des effets potentiels importants, qui constituent une menace extérieure pour l'Union ou ses États membres ».

Le point 2 précise que « les cyberattaques constituant une menace extérieure sont notamment celles qui : a) ont leur origine ou sont menées à l'extérieur de l'Union ; b) utilisent des infrastructures situées à l'extérieur de l'Union ; c) sont menées par toute personne physique ou morale, toute entité ou tout organisme établi ou agissant à l'extérieur de l'Union ; ou d) sont menées avec l'appui, sur les instructions ou sous le contrôle de toute personne physique ou morale, entité ou organisme agissant à l'extérieur de l'Union. »

Enfin, le point 3 nous dit que « les cyberattaques sont des actions faisant intervenir l'un ou l'autre des éléments suivants : a) l'accès aux systèmes d'information ; b) les atteintes à l'intégrité d'un système d'information ; c) les atteintes à l'intégrité des données ; ou d) l'interception de données, lorsque ces actions ne sont pas dûment autorisées par le propriétaire du système ou des données ou d'une partie du système ou des données ou par une autre personne détenant des droits sur le système ou les données ou une partie du système ou des données, ou sont en contravention avec le droit de l'Union ou de l'État membre concerné ».

1. Art. 1 (3) de la loi du 27 octobre 2010 relative à la mise en œuvre de résolutions du Conseil de sécurité des Nations Unies et d'actes adoptés par l'Union européenne comportant des interdictions et mesures restrictives en matière financière à l'encontre de certaines personnes, certaines entités et certains groupes dans le cadre de la lutte contre le financement du terrorisme.

Le point suivant présente quelques exemples de cyberattaques constituant une menace pour les États de l'Union ; il s'agit de celles qui toucheraient aux infrastructures critiques comme les câbles sous-marins, ou aux services nécessaires au maintien de l'activité sociale et économique, ou encore aux fonctions critiques de l'État notamment en matière de défense.

Enfin, pour déterminer si une cyberattaque a un effet important, les facteurs suivants sont pris en considération par l'article 3 : « a) la portée, l'ampleur, l'incidence ou la gravité des perturbations causées, notamment sur les activités économiques et sociétales, les services essentiels, les fonctions critiques de l'État, l'ordre public ou la sécurité publique ; b) le nombre de personnes physiques ou morales, d'entités ou d'organismes touchés ; c) le nombre d'États membres concernés ; d) l'ampleur des pertes économiques causées, notamment par le pillage de fonds, de ressources économiques ou de propriété intellectuelle ; e) l'avantage économique acquis par l'auteur de l'infraction, à son profit ou au profit de tiers ; f) la quantité ou la nature des données volées ou l'ampleur des violations de l'intégrité des données ; ou g) la nature des données sensibles sur le plan commercial auxquelles il a été accédé. »

Avec les articles 4 et 5, le couperet tombe : les personnes listées sont interdites de territoire sur l'ensemble des États membres, que ce soit pour un séjour ou un simple transit et tous leurs avoirs sont gelés.

L'article 6 prévoit que les noms figurant sur la liste sont choisis ainsi : « Le Conseil, statuant à l'unanimité sur proposition d'un État membre ou du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, établit la liste qui figure à l'annexe et la modifie. »

La dernière décision PESC du 30 juillet 2020 modifiant celle de mai 2019 et mise en œuvre par le règlement d'exception (UE) 2020/1125 du Conseil du 30 juillet 2020 énonce pour la première fois neuf noms que nous retrouvons aujourd'hui dans la liste française de gel des avoirs.

Ces noms sont tout aussi étonnants que cette nouvelle sanction ; les voici, selon la dernière mise à jour du règlement du 20 novembre 2020[2] :

1. Centre principal des technologies spéciales (GTsST) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU).
2. 85e Centre principal des services spéciaux (GTsSS) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU).
3. Chosun Expo.
4. Tianjin Huaying Haitai Science and Technology Development Co. Ltd.
5. SOTNIKOV Oleg Mikhaylovich.
6. SEREBRIAKOV Evgenii Mikhaylovich.

7. MORENETS Aleksei Sergeyvic.
8. MININ Alexey Valeryevich.
9. ZHANG Shilong.
10. GAO Qiang.
11. BADIN Dmitry Sergeyevich.
12. KOSTYUKOV Igor Olegovich.

Le premier est le plus étonnant, et il y a de quoi faire frisonner : il y a moins de 100 ans en arrière, il en fallait bien moins pour déclencher une guerre mondiale.

Et pourtant, il est aujourd'hui reproché au Centre principal des technologies spéciales (GTsST) de la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GU/GRU) sa responsabilité dans de nombreuses cyberattaques. Sont citées « les cyberattaques de juin 2017 connues sous les noms de "NotPetya" ou "Eternal-Petya" et les cyberattaques lancées contre un réseau électrique ukrainien pendant l'hiver 2015-2016 ».

Cette découverte soulève bien des questionnements. Comment les États membres collaborent-ils à la construction de cette liste ? Les cyberattaques sont-elles donc considérées comme étant tout aussi dangereuses qu'une attaque terroriste ? L'ONU prendra-t-elle aussi des mesures en la matière ? Comment les services de renseignement travaillent-ils sur ces phénomènes ? La coopération entre les États est-elle vraiment effective sur ces sujets ?

Plus encore, cette sanction est-elle une arme de plus dans une guerre économique, une guerre *cyber* qui est, à mon sens, la nouvelle forme de guerre mondiale à laquelle nous devons nous préparer ?

Affaire à suivre…

2. Règlement d'exécution (UE) 2020/1744 du Conseil du 20 novembre 2020 mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres.