Cyberattaques : vers une nouvelle obligation d'annonce

Célian Hirsch, le 28 décembre 2022

Le 2 décembre 2022, le Conseil fédéral a proposé au Parlement d'introduire une obligation de signaler les cyberattaques dans les 24 heures au Centre national suisse pour la cybersécurité.

En raison de l'augmentation de cyberattaques, le Conseil fédéral désire octroyer au Centre national suisse pour la cybersécurité (NCSC) une vue d'ensemble des cybermenaces en Suisse. Avec une telle connaissance, le NCSC pourrait avertir les victimes potentielles et leur recommander les mesures qui s'imposent (art. 74*a* al. 4 du projet de Loi sur la sécurité de l'information [P-LSI]).

À l'heure actuelle, le NCSC ne reçoit des informations que sur une base volontaire. Or, une vue d'ensemble n'est possible que si toutes les infrastructures critiques lui annoncent les cyberattaques d'une certaine importance (art. 74*d* P-LSI). L'obligation s'appliquerait ainsi à certaines infrastructures critiques, dont feraient partie notamment les hautes écoles, l'administration tant fédérale, cantonale que communale, les entreprises énergétiques, les banques, assurances et infrastructures des marchés financiers, ou encore les hôpitaux, la SSR, la Poste, les CFF, ainsi que les prestataires *cloud* sis en Suisse, voire encore certains fabricants de logiciels (art. 74*b* P-LSI). En raison de cette large liste, le Conseil fédéral pourrait exempter certaines infrastructures critiques de l'obligation de signaler, lorsque les cyberattaques n'auraient qu'un effet limité sur le fonctionnement de l'économie ou sur le bien-être de la population (art. 74*c* P-LSI).

La cyberattaque devrait être annoncée uniquement si l'une des quatre conditions suivantes est remplie (conditions alternatives, art. 74*d* P-LSI) :

1. la cyberattaque met en péril le fonctionnement de l'infrastructure critique concernée ;
2. la cyberattaque a entraîné une manipulation ou une fuite d'informations ;
3. la cyberattaque n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou
4. la cyberattaque s'accompagne d'actes de chantage, de menaces ou de contrainte.

L'infrastructure critique devrait informer le NCSC dans les 24 heures suivant la détection de la cyberattaque (art. 74*e* al. 1 P-LSI). L'information devrait comprendre des informations sur l'autorité ou l'organisation assujetties à l'obligation de signaler, sur le type et l'exécution de la cyberattaque, sur ses effets, sur les mesures prises et, si elles sont connues, sur les mesures prévues (art. 74*e* al. 2 P-LSI).

Afin de respecter le principe *nemo tenetur* (nul n'est tenu de s'auto-incriminer), l'infrastructure critique ne serait pas obligée de communiquer au NCSC des informations qui l'exposeraient à des poursuites pénales (art. 74*e* al. 4 P-LSI). Par ailleurs, les informations remises au NCSC seront expressément exclues du champ de la Loi sur la transparence (art. 4 al. 1bis P-LSI).

Afin que cette future obligation d'annonce soit respectée, le Conseil fédéral propose tant une incitation positive que négative. La première consisterait dans le soutien que le NCSC apportera aux infrastructures critiques suite à une cyberattaque (art. 74 P-LSI). La seconde consisterait en une potentielle amende de CHF 100'000. Celle-ci ne s'appliquerait que lorsque l'assujetti persiste à ne pas respecter son devoir, après avoir (1) été rendu attentif à son devoir de signaler la cyberattaque et (2) s'être vu octroyer un ultime délai pour le respecter (art. 74*g cum* art. 74*h* P-LSI). Malgré certaines critiques lors de la procédure de consultation, cette mesure *ultima ratio* nous semble nécessaire. Elle correspond d'ailleurs à la pratique générale qu'une décision d'une autorité administrative peut être rendue avec la menace d'une amende pénale.

Ce projet de loi constitue-t-il un premier pas vers une loi plus générale imposant aux infrastructures critiques des exigences minimales en matière de cybersécurité ? Le Conseil fédéral ne l'indique pas expressément, mais vu l'importance grandissante de la cybersécurité depuis quelques années, une telle évolution ne nous semble pas exclue. Tel est d'ailleurs déjà le cas dans l'Union européenne depuis 2018 avec la directive NIS, dont la version révisée (NIS2) a été adoptée le 14 décembre 2022.

Proposition de citation : Célian Hirsch, Cyberattaques : vers une nouvelle obligation d'annonce, 28 décembre 2022 *in* www.swissprivacy.law/193