

## Gestion de cyberincidents et infrastructures critiques : analyse du cadre légal

Thèse de droit suisse - Présentation

Pauline MEYER

La cybersécurité est aujourd'hui une préoccupation majeure pour l'ensemble de la société. Il est nécessaire d'inciter les organisations à assurer un niveau de cybersécurité approprié pour gérer efficacement les cyberattaques, autres cyberincidents et vulnérabilités susceptibles de les compromettre. Essentielles à la population et au fonctionnement de la société, les infrastructures critiques doivent en particulier se saisir de cette problématique transversale. Tous les leviers à disposition doivent être mobilisés pour parvenir à cette fin, dont le droit. La thèse analyse le cadre légal suisse actuellement applicable aux infrastructures critiques dans ce domaine et émet des propositions de développement pour améliorer la législation en vigueur.

La cybersécurité est cruciale non seulement dans le domaine technique mais aussi dans les domaines juridique, éthique et politique, surtout lorsqu'il en va de la cybersécurité au sein des infrastructures critiques, qui fournissent des services essentiels au bien-être de la population, au fonctionnement de la société ou à l'économie nationale et qui constituent par conséquent l'un des groupes cibles clés pour assurer la résilience d'un État. Bien qu'une législation suisse en matière de cybersécurité applicable aux infrastructures critiques commence à se développer, elle est encore insuffisante, lacunaire et dispersée. Les infrastructures critiques méritant une protection spéciale en raison principalement de leur importance pratique, il convient aujourd'hui de se saisir davantage de cette problématique. Il est nécessaire de trouver la bonne réglementation pour ce domaine et ces parties prenantes, afin de respecter et concilier tous les principes et les droits présents tout en disposant d'une réglementation efficace et efficiente.

Pour assurer un bon niveau de cybersécurité, le droit doit être mobilisé conjointement aux autres leviers d'action à disposition. Il participe à l'introduction et à l'implémentation d'exigences de cybersécurité et de gestion de cyberincidents, ainsi qu'à la codification



d'enjeux et de principes. Les défis auxquels est confrontée la réglementation d'un tel domaine sont nombreux et relèvent notamment de la subsidiarité de l'intervention étatique et des réglementations sectorielles. Ils proviennent également de la diversité d'acteurs et de pratiques à cerner ou du caractère évolutif des technologies de l'information et de la communication.

La thèse compte répondre à plusieurs questions. Il est tout d'abord essentiel de définir les notions centrales dans le cadre de la protection contre les cyberrisques et plus particulièrement dans le domaine de la cybersécurité. Il convient également d'aborder la diversité d'instruments politiques entourant la législation ainsi que la diversité d'acteurs et parties prenantes dans le domaine en Suisse, dans le public comme dans le privé. Ensuite, le cadre légal en Suisse régissant la cybersécurité et la gestion de cyberincidents auprès des différents secteurs et sous-secteurs critiques doit être analysé, en prenant en considération les différentes spécificités comme les éléments transversaux ainsi que la législation dans les autres domaines de la protection contre les cyberrisques, à savoir la cybercriminalité et la cyberdéfense. Finalement, la thèse soulève les lacunes que l'on peut observer en droit suisse et suggère des alternatives pour pallier ces lacunes et réglementer de la façon la plus satisfaisante la cybersécurité et la gestion de cyberincidents au sein des infrastructures critiques en Suisse.

### **Contexte de la thèse**

La thèse est rédigée dans le cadre d'un projet financé par le Fonds national suisse (FNS). Le projet NRP-77 « *Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland* » permet la coopération entre l'Université de Lausanne (UNIL), l'Université de Zurich (UZH) et le Centre national pour la cybersécurité (NCSC).

Le projet - et la thèse rédigée dans ce contexte - a débuté début 2021 et s'achèvera début 2024. Il analyse le cadre légal en matière de cybersécurité et de gestion de cyberincidents en droit suisse et à formuler des propositions de modifications législatives. En même temps, le projet doit établir quels sont les besoins des parties prenantes - particulièrement des infrastructures critiques et des équipes de gestion de cyberincidents -, les obstacles auxquels elles sont confrontées et les questions de leur quotidien pour formuler, en parallèle des propositions législatives, des propositions de lignes directrices pour appréhender les différents enjeux juridiques et éthiques.