COMPTE RENDU NON THÉMATIQUE

LÉONETTI Xavier, 2015, *Guide de cybersécurité. Droits, méthodes et bonnes pratiques*. Paris, L'Harmattan, 322 p. (Alban Thomas)

Docteur en droit, chargé de cours dans plusieurs universités, officier de gendarmerie et directeur du service d'« intelligence économique » de gendarmerie, Xavier Léonetti est un spécialiste reconnu de la cybercriminalité. Auteur du *Guide de cybercriminalité. Droits, méthodes et bonnes pratiques* qui a reçu le prix littéraire de l'Institut national des hautes études de sécurité et de justice (INHESJ) un an après sa publication, Léonetti est donc un acteur de premier plan dans la lutte de la cybercriminalité française et partage ses connaissances dans un recueil de conseils et d'explications sur les enjeux qui touchent de près ou de loin à la cybercriminalité.

Le côté « guide encyclopédique » de l'ouvrage est renforcé tout au long du livre par une construction particulière des chapitres. Après une introduction qui met en place la situation actuelle des enjeux de la cybercriminalité au moyen de statistiques, le livre est séparé en deux parties. La première consiste à définir tout le langage informatique dont le lecteur a besoin pour poursuivre sa lecture. « Wi-Fi », « Adresse IP », « Navigateur Internet », « Anti-virus » font partie des concepts définis dans les deux premiers chapitres. À la manière d'un dictionnaire, ce guide fournit des définitions précises pour aborder en toute clarté à la fois l'informatique et les enjeux cybercriminels. La deuxième partie dresse un panorama de la cybercriminalité, en abordant les thèmes comme les cybermenaces, le sentiment de cyber-insécurité, les mesures de cybercriminalité et les moyens de lutter contre elle. Le dernier chapitre est un peu à part : il fait office de conclusion en résumant l'ouvrage d'une façon didactique. Offrant « 10 conseils de "cyber-bon sens" » (p. 287) et pointant du doigt les bons réflexes à adopter, ce chapitre constitue à la fois un résumé très concis de l'ouvrage mais aussi un recueil de conseils pour les gros réseaux informatiques en entreprise tout autant que pour les utilisateurs ordinaires. Ces conseils vont de « Payer en toute sécurité » à « En cas de problème, appeler à l'aide » (p. 292) avec les références complètes de l'Agence nationale de la sécurité des systèmes d'information en France.

Enfin, l'ouvrage met un point d'honneur à illustrer ses propos à l'aide d'exemples tout au long des chapitres, exemples partagés en quatre catégories : les « Compléments d'enquêtes », les « RETour d'EXpérience », les « Ce que dit la loi » et « Ce que dit la jurisprudence ». Les « Compléments d'enquêtes » sont des retours explicatifs qui ne pourraient pas s'imbriquer naturellement dans le texte et servent à définir des structures administratives ou des pratiques spécifiques. Les « RETour d'EXpérience » sont un concept tiré de l'enseignement du commandement militaire. Les RETEX sont des retours sur des évènements passés pour en tirer des leçons tout en illustrant le sujet enseigné. Ils permettent aussi d'ancrer les exemples dans la réalité puisque ce sont toujours des évènements réels accompagnés de dates. Les « Ce que dit la loi » et « Ce que dit la jurisprudence » se ressemblent beaucoup et permettent à l'auteur de citer explicitement des articles de lois ou des jurisprudences pour étayer ses propos. Ces encarts permettent au lecteur de bien comprendre le texte sans avoir à chercher des informations complémentaires.

En voulant dresser un panorama de la cybercriminalité, le livre s'attelle donc à définir toutes les sortes de menaces, allant du « *phising* » (filoutage) aux « attaques DDOS ». En voulant

aller plus loin et en se basant sur les travaux du CLUSIF (Club de la sécurité de l'information français) et de l'ANSSI (Agence nationale de la sécurité des systèmes d'information), l'ouvrage s'attelle à détailler une « échelle de Richter des cybermenaces » (p. 202). Créant ainsi une gradation entre les menaces selon des critères précis, cette échelle à l'utilisateur de mieux s'y retrouver puisque pour chaque menace, « les cibles, les auteurs potentiels et les méthodes d'attaques » sont décrits. Cette échelle est aussi utile pour forcer les organismes de cyber sécurité à effectuer un recensement rigoureux des menaces portant sur les systèmes informatiques.

Le *Guide de cybersécurité…* n'est donc pas un ouvrage théorique qui amènerait l'auteur à développer une réflexion particulière. La force de l'ouvrage est de donner au lecteur les clés qui mènent à une compréhension plus fine des enjeux de la cybercriminalité. Cela passe par la compréhension des mécanismes de la justice mais aussi par un éclaircissement du monde informatique parfois compliqué et truffé de concepts ésotériques.

Alban Thomas
Département de sociologie
Université de Montréal, Montréal (Québec), Canada