[LU] Ratification de la Convention du Conseil de l'Europe sur la cybercriminalité

IRIS 2014-10:1/24

Mark D. Cole & Jenny Metzdorf
Université du Luxembourg

Le 18 juillet 2014, le Grand-Duché de Luxembourg a officiellement ratifié et mis en œuvre la Convention du Conseil de l'Europe sur la cybercriminalité, ainsi que son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Le Grand-Duché était, en effet, l'un des derniers membres du Conseil de l'Europe à avoir signé en 2003 la Convention et son Protocole, sans l'avoir encore ratifiée ; la Chambre des Députés avait fait l'objet de pressions en ce sens par un certain nombre d'organisations internationales.

Le Luxembourg avait déjà mis en place dans son droit pénal, avant qu'internet n'ait pris une importance accrue, des dispositions relatives aux attaques commises contre les systèmes informatiques. La plupart des dispositions contenues dans la Convention qui portent sur ces aspects de fond ont déjà été transposées par le législateur luxembourgeois et ne nécessitent, par conséquent, aucune autre modification. Cela concerne, par exemple, les infractions prévues par la Convention en matière de pornographie enfantine : l'article 383ter du Code pénal luxembourgeois prévoit déjà, notamment, une disposition étendue selon laquelle le stockage ou la transmission en vue de sa diffusion par quelque moyen que ce soit, d'une image de pornographie enfantine constitue une infraction pénale.

De même, l'objectif du Protocole additionnel à la Convention, qui vise à harmoniser le « droit pénal matériel dans la lutte contre le racisme et la xénophobie sur internet » et à améliorer la « coopération internationale dans ce domaine » avait déjà été atteint au Luxembourg : le code pénal luxembourgeois prévoit déjà ces infractions, comme la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques, énoncée à l'article 3 du Protocole, qui correspond à l'article 457-1 du Code pénal. Cette disposition interdit toute incitation à la haine et à la violence contre une personne ou un groupe de personnes par tout moyen écrit, parlé ou pictural fondé sur l'un des éléments énoncés à l'article 454 du Code pénal. L'article 454 va même plus loin que la liste figurant à l'article 2 du Protocole, puisqu'il englobe non seulement l'origine, la couleur de peau, l'ascendance, l'appartenance nationale ou ethnique et la religion, mais également les attaques perpétrées contre des individus ou des groupes de personnes en raison de leur orientation sexuelle, leur sexe, leur

© Observatoire européen de l'audiovisuel (Conseil de l'Europe) 2025

handicap, ainsi que leur âge.

Cependant, cette loi de ratification vise à combler certaines lacunes du droit positif national, en tenant compte de la jurisprudence nationale. Cela concerne tout particulièrement les dispositions pénales applicables aux infractions en matière de protection des données. La loi du 18 juillet 2014 modifie un certain nombre de dispositions du Code pénal et du Code d'instruction criminelle. L'article 496 du Code pénal énonce, par exemple, désormais de manière explicite les clefs électroniques et les mots de passe parmi les objets que l'auteur de l'infraction peut chercher à obtenir, car il était auparavant impossible d'incriminer le fait d'utiliser frauduleusement le mot de passe d'une personne ou d'usurper en ligne l'identité d'autres personnes qui utilisaient leur véritable nom.

De manière encore plus importante, des dispositions procédurales ont été ajustées, afin de tenir compte des exigences de la Convention. Ainsi, afin de satisfaire au Titre 2 de la Convention relatif à la conservation rapide de données informatiques stockées, une importante modification concerne l'article 24-1, alinéa 1 du Code d'incrimination pénale, qui met en place une « procédure de blocage rapide des données ». Selon cette procédure, il sera possible de suivre et de localiser l'origine ou la destination des données sans pour autant devoir procéder immédiatement à l'ouverture d'une enquête préliminaire. Il faudra par conséquent imposer aux fournisseurs, moyennant un préavis spécifique, de conserver l'ensemble des données disponibles sur un utilisateur ou sur un compte spécifique et de les tenir à disposition pour toute éventuelle autre demande émanant de l'autorité compétente pour le traitement de ces données. Ainsi, de précieuses informations susceptibles d'être perdues ou modifiées pourraient être tenues à disposition pour une durée de 90 jours, à la demande du juge d'instruction ou du procureur général. Enfin, les modifications nécessaires découlant des changements mentionnés ci-dessus sont également mises en place par la loi relative à la protection des données dans le domaine des communications électroniques.

Loi du 18 juillet 2014 portant 1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, 2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, 3) modification du Code pénal, 4) modification du Code d'instruction criminelle, 5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, Mémorial A - N° 157, 12 août 2014, page 2406

http://www.legilux.public.lu/leg/a/archives/2014/0157/a157.pdf

© Observatoire européen de l'audiovisuel (Conseil de l'Europe) 2025

© Observatoire européen de l'audiovisuel (Conseil de l'Europe) 2025