

La loi LEN trouble certains experts en sécurité

A peine la LEN (ou loi pour la confiance dans l'économie numérique) est-elle adoptée, qu'elle suscite à nouveau des remous. Un consultant, spécialisé en sécurité, observe que la modification de l'article 323-3 du code pénal est effective avec l'adoption de l'article 34 de la nouvelle loi: Le nouvel article »

concerne tous les experts en sécurité informatique, consultants, chercheurs de failles, ou journalistes /rédacteurs de magazines spécialisés: il n'est plus possible de publier les détails techniques d'une vulnérabilité, publier ou manipuler des outils permettant les tests intrusifs ou les audits de sécurité ... sans être en situation illégale ! » Extrait: « **Art. 323-3-1.** – Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.» Le même consultant relève que l'on a introduit une expression, « subjective » où il s'agit de justifier un « sans motif légitime »... « Toute personne manipulant des outils de sécurité, ou publiant des détails techniques devient coupable jusqu'à ce qu'elle prouve son innocence (à la personne de prouver que son motif est « légitime »). La présomption d'innocence est donc remplacée par la présomption de culpabilité« . Notre expert ajoute: « Quel avenir pour le 'full-disclosure' en France ? Faut-il arrêter les conférences sur la sécurité ? Faut-il arrêter les tests d'intrusions ? Faut-il accepter l'insécurité ? Ou faut-il tout simplement se délocaliser ? », interroge Fabien X., consultant en sécurité (K-OTik Security Staff, www.k-otik.com).