



Luxembourg, le 30 mai 2014

Réf : 2014/15077/288

CHAMBRE DES DÉPUTÉS  
Entrée le:  
04 JUIN 2014

A  
Monsieur le Ministre  
aux Relations avec le Parlement  
p.a. Service Central de Législation  
L-2450 Luxembourg

**Objet :** Question parlementaire n°244 du 29 avril 2014 de Madame la Députée Nancy ARENDT.

Monsieur le Ministre,

J'ai l'honneur de vous transmettre ci-joint la réponse à la question parlementaire reprise sous rubrique.

Je vous prie de croire, Monsieur le Ministre, à l'expression de mes sentiments très distingués.

Ministère aux Relations avec le Parlement  
SERVICE CENTRAL DE LEGISLATION

N° :	SCL :
Reçu le :	4 JUIN 2014

Le Ministre de la Sécurité Intérieure,

  
Etienne Schneider

**Réponse du Ministre de la Sécurité Intérieure et du Ministre de la Justice à la question parlementaire n° 244 du 29 avril 2014 de l'honorable Députée Nancy Arendt**

Il est vrai qu'une nouvelle forme de délinquance a fait son apparition ces dernières années. Celle-ci est liée à l'usage abusif de photos et/ou films enregistrés à l'insu de la victime au cours d'une conversation par ordinateur.

Entre janvier 2013 et mai 2014 une quarantaine de faits ont été portés à la connaissance du parquet de Diekirch. Le nombre d'infractions dans ce domaine est certainement plus important étant donné que certaines victimes préfèrent ne pas porter plainte de peur de s'exposer au ridicule.

La Police grand-ducale a enregistré 80 plaintes en 2013.

Le mode opératoire type peut être décrit comme suit : une personne, le plus souvent de sexe masculin, accède à un des multiples sites de rencontres en ligne et engage un contact avec une personne du sexe opposé. Après un échange de quelques messages écrits, le correspondant de la future victime invite cette dernière à continuer le contact sur une plateforme de télécommunication visuelle par internet du type Skype, FaceTime ou autres. C'est alors que la conversation s'oriente peu à peu vers un terrain plus intime, et à un certain moment, il est proposé à la victime de se dénuder devant sa WEBCAM, comportement que son correspondant enregistre à son insu. Peu après, la victime est harcelée par des messages la menaçant que, faute de paiement d'une certaine somme d'argent, des photos ou extraits de films enregistrés seront diffusés sur un des sites sociaux.

Il est très difficile de lutter efficacement contre ce genre de criminalité pour les raisons suivantes :

- les auteurs n'agissent pas depuis le Luxembourg, mais sont le plus souvent établis à l'étranger ;
- il n'est pas évident d'obtenir, de la part des autorités judiciaires de pays limitrophes, les données relatives à l'identification des utilisateurs d'une adresse IP puisque, par exemple en Allemagne, la législation nationale ne permet plus aucune sauvegarde des données de connexion (Vorratsdatenspeicherung). L'information ne peut partant être obtenue qu'à condition de se montrer extrêmement rapide et d'agir dans les 7 à 10 jours à partir de la connaissance des faits, c'est-à-dire endéans le délai au cours duquel l'opérateur stocke les données en vue de la facturation du service à son client ;
- il faut noter que les délinquants informatiques ne font que très rarement usage de leur propre accès internet, mais opèrent souvent à partir de structures comme les « cyber-cafés », sinon utilisent un accès internet par un téléphone mobile qui, pour des raisons techniques, ne permet pas une identification par une adresse IP individualisable ;
- le paiement de la rançon dans ce genre de criminalité se fait généralement par la voie de WESTERN UNION, service offert par la Poste qui permet un transfert extrêmement rapide de sommes d'argent d'une façon tout à fait anonyme à travers le monde entier. Retrouver dans ce cas de figure le bénéficiaire relève du pur hasard.

En admettant enfin qu'un délinquant établi à l'étranger puisse être identifié, traduire celui-ci devant les juridictions luxembourgeoises pose encore un autre problème procédural. En effet, en cas de refus de celui-ci de se présenter devant le juge d'instruction sur mandat de comparution, toute inculpation s'avère difficile, voire impossible et la procédure reste bloquée à ce stade, à moins de délivrer un mandat d'arrêt européen, sinon international, ce qui est toutefois le plus souvent disproportionné au vu de l'envergure de l'affaire.

Les poursuites s'avèrent dès lors difficiles en cette matière mais il faut espérer que les gens sont entretemps informés de cette pratique et des risques qu'elle comporte.

Les textes légaux existants dont l'article 470 du Code pénal ainsi que les dispositions de la loi du 11 août 1982 concernant la protection de la vie privée, sont suffisants pour réprimer cette nouvelle sorte de comportement délictuel, à condition de pouvoir identifier l'auteur et de le faire comparaître utilement devant les juridictions nationales.

Il faut souligner également que la Chambre des Députés va voter prochainement le projet de loi n°6514 portant approbation de la Convention du Conseil de l'Europe sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001 et portant modifications de différents textes. Ce projet de loi complète notre arsenal législatif en matière de lutte contre la cybercriminalité sur plusieurs points.

Finalement, il faut souligner l'importance d'une sensibilisation adéquate du public afin de le rendre conscient des dangers de telles pratiques et de la possibilité d'un enregistrement à tout moment.