OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

IRIS

Rechtliche Rundschau der
Europäischen Audiovisuellen Informationsstelle

IRIS 2014-10/24

LU-Luxemburg:Übereinkommen des Europarats zur Computerkriminalität ratifiziert

Am 18. Juli hat das Großherzogtum Luxemburg das Cybercrime-Übereinkommen des Europarats offiziell ratifiziert und umgesetzt; dies gilt auch für das Zusatzprotokoll betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art. Da das Großherzogtum eines der letzten Mitglieder des Europarats war, das das Übereinkommen und das Zusatzprotokoll unterzeichnet (2003) aber nicht ratifiziert hat, sah sich das Parlament (Chambre des Députés) dem Druck seitens einer Reihe internationaler Organisationen ausgesetzt.

Luxemburg hatte bereits zu einem frühen Zeitpunkt, Regelungen betreffend Angriffe auf Informationssysteme in das Strafrecht aufgenommen. Das Internet hatte damals noch nicht die Bedeutung, die es heute hat. Damit hat der luxemburgische Gesetzgeber die Mehrzahl der in dem Übereinkommen enthaltenen Bestimmungen zu wesentlichen Aspekten bereits umgesetzt, und Änderungen waren nicht erforderlich. Dies gilt z.B. für den in dem Übereinkommen vorgesehenen Straftatbestand hinsichtlich Kinderpornographie: Art. 833ter des luxemburgischen Strafgesetzbuchs sieht u.a. bereits eine umfangreiche Bestimmung vor, nach der es strafbar ist, pornografische Bilder von Minderjährigen zum Zweck der Weiterverbreitung - unahängig von deren Art - zu speichern oder zu übermitteln.

Auch das im Zusatzprotokoll zum Übereinkommen genannte Ziel, die „materiellrechtlichen Vorschriften zur Bekämpfung rassistischer und fremdenfeindlicher Propaganda zu harmonisieren“ und die internationale Zusammenarbeit in diesem Bereich zu verbessern, hat Luxemburg bereits erreicht: das Strafgesetzbuch deckt diese Straftaten ab; so entspricht z.B. Art. 3 des Protokolls „Verbreitung rassistischen und fremdenfeindlichen Materials über Computersysteme“ dem Art. 457-1 des Luxemburger Strafgesetzbuchs. Die Bestimmungen verbieten den Aufruf zu Hass und Gewalt gegen eine Person oder eine Gruppe in schriftlicher, mündlicher oder bildlicher Form aufgrund der in Art. 454 des Strafgesetzbuchs genannten Kriterien. Art. 454 geht sogar über die in Art. 2 des Protokolls enthaltene Liste hinaus, indem hier nicht nur von Rasse, Hautfarbe, Abstammung, nationaler oder ethnischer Herkunft und Religion die Rede ist, sondern auch von Angriffen auf Einzelpersonen oder Gruppen wegen ihrer sexuellen Orientierung, ihres Geschlechts, ihrer Behinderung und ihres Alters.

Das Ratifizierungsgesetz schließt jedoch auch einige Lücken im nationalen materiellen Recht und berücksichtigt die ständige Rechtsprechung in Luxemburg. Dies gilt im Besonderen für die strafrechtlichen Bestimmungen bei Verstößen gegen den Datenschutz. Das Gesetz vom 18. Juli 2014 novelliert eine Reihe von Bestimmungen des Strafgesetzbuchs und der Strafprozessordnung. Nach Art. 496 des Strafgesetzbuchs z.B. zählen nunmehr elektronische Schlüssel und Passwörter ausdrücklich zu den Gegenständen, die sich Straftäter zu beschaffen versuchen; denn vorher war es nicht möglich, das „Passwort-Phishing“, den „Diebstahl“ von „Online-Identitäten“ anderer Personen unter Strafe zu stellen, wenn dabei authentische Namen verwendet wurden.

Sehr wichtig ist noch der Hinweis, dass die Prozessordnung angepasst wurde, um den Anforderungen des Übereinkommens zu genügen. In Bezug auf Titel 2 des Übereinkommens - Umgehende Sicherung gespeicherter Computerdaten - besteht eine der wichtigen Änderungen in Art. 24-1 Punkt 1 der Strafprozessordnung in der Einführung des “Quick Freeze”-Verfahrens. Mit diesem Verfahren wird es möglich sein, die Quelle bzw. das Ziel von Verbindungsdaten auszumachen und zu lokalisieren, ohne dass dazu ein vorläufiges Verfahren eröffnet werden muss. Dies wird dadurch ermöglicht, dass der Provider durch eine entsprechende Mitteilung aufgefordert werden kann, sämtliche verfügbaren Daten eines bestimmten Nutzers bzw. eines Kontos zu speichern und die Daten für eventuelle spätere offizielle Anfragen von zuständigen Stellen bereitzuhalten bzw. zu übergeben. Auf diese Weise können nützliche Informationen, die verloren gehen oder verändert werden können, auf Veranlassung des Ermittlungsrichters oder der Staatsanwaltschaft für einen Zeitraum von 90 Tagen bereitgehalten werden. Schließlich war es aufgrund der vorgenannten Änderungen notwendig, die Datenschutzgesetze für den Sektor elektronische Kommunikation zu novellieren.

• *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* (Gesetz vom 18. Juli 2014 über das Übereinkommen über Computerkriminalität des Europarats, das Zusatzprotokoll und andere Änderungen; Memorial A - N°157 vom 12. August 2014, S. 2406)
http://merlin.obs.coe.int/redirect.php?id=17260

FR

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL
EUROPEAN AUDIOVISUAL OBSERVATORY
EUROPÄISCHE AUDIOVISUELLE INFORMATIONSSTELLE

IRIS

Rechtliche Rundschau der
Europäischen Audiovisuellen Informationsstelle

Mark D. Cole & Jenny Metzdorf

Universität Luxemburg