forumpoenale Stämpfli Verlag

forumpoenale 6/2018 | S. 469–469 469

Editorial

«Es rollt ein digitaler Tsunami auf uns zu»

Liebe Leserinnen, liebe Leser,

Mit diesem bedrohlichen Bild des «digitalen Tsunamis» forderte jüngst kein Geringerer als der künftige ETH-Präsident, Professor Dr. Joël Mesot, weitere Anstrengungen im Bereich der Digitalisierung. Was für die Forschung gilt, gilt für die Strafrechtspraxis ebenso. Während die Wirtschaft sowie ausländische politische und wirtschaftliche Nachrichtendienste Milliarden in die Digitalisierung investieren, stellt sich die schweizerische Strafrechtswelt dieser Herausforderung nur allzu zögerlich. Dabei ist schon die Alltagskriminalität längst «digitalisiert». Täter drohen etwa mit der Veröffentlichung von manipulierten pornografischen Bildern oder damit, im Namen ihrer Opfer betrügerische Internetanzeigen zu schalten oder Daten zu vernichten. Gefordert wird dabei zeitgleich eine Erpressungssumme, sonst würden die Opfer sozial und psychisch zerstört.

Die Cyberkriminellen agieren grenzenlos, hinterlassen Hunderte von Opfern in allen Teilen der Schweiz, operieren oft aus dem Ausland und kaschieren ihre Spuren im Nu. Die Strafverfolgung dagegen stösst überall an Grenzen – räumlich, personell und mit Blick auf die rechtlichen Möglichkeiten. Es fehlt teils auch an Fachwissen und den notwendigen technischen Ermittlungstools. Grenzenlosigkeit und Grenzhaftigkeit stehen sich hart gegenüber. Vorschnelle politische Forderungen nach mehr Effizienz bringen indes nichts. Gefordert sind vor allem Investitionen. Man muss Geld in die Hand nehmen – Geld, das später an einem anderen Ort möglicherweise fehlen würde. Solche Umverteilungen erfolgen selten reibungslos. Zudem müssen die Polizeikorps und Staatsanwaltschaften die Cybercrime-Zuständigkeit an neu zu planende Landesregionen oder den Bund abgeben. Hier dürfte sich die Einsicht mehr und mehr durchsetzen, dass ein «Zuviel» an Verantwortung über kurz oder lang zur lähmenden Belastung wird.

Zur Stärkung des Know-hows *bei Staatsanwaltschaften, Gerichten und der Polizei startet die Staatsanwaltsakademie 2019 mit einem 3-stufigen Ausbildungskonzept bzw. den Cybercrime-Kursen I–III. Der Start legt ein Grundkurs zur sog. digitalisierten Alltagskriminalität, welche die IT als Tat- und Beweismittel einsetzt. Ein Kurs zum materiellen und formellen Cybercrime-Strafrecht und ein Hightech-Crime-Kurs speziell für strafbehördliche Spezialisten auf höchstem Niveau werden folgen. Möge die Strafverteidigung bald ähnliche Kurse anbieten, denn die Qualität eines Prozesses gewinnt mit dem* Know-how *aller.*

Frohe Festtage

«Un tsunami digital se dirige vers nous»

Chères lectrices, chers lecteurs,

A l'aide de cette image menaçante du «tsunami digital», le professeur Joël Mesot, président désigné de l'EPFZ, a récemment exigé de nouveaux efforts dans le domaine de la digitalisation. Ce qui vaut pour la recherche s'applique également à la pratique pénale. Tandis que l'économie et les services étrangers de renseignements politiques et économiques investissent des milliards dans la digitalisation, le monde pénal suisse relève ce défi de manière bien trop hésitante. Même la délinquance quotidienne est pourtant «digitalisée» depuis longtemps. Les auteurs menacent par exemple de publier des images pornographiques manipulées ou, au nom de leurs

victimes, de placer sur internet des annonces trompeuses ou d'effacer des données; leur but est d'extorquer de l'argent à des personnes que la crainte d'un anéantissement social et psychique doit amener à céder.

Les cybercriminels opèrent par-dessus les frontières, engendrent des centaines de victimes partout en Suisse, agissent souvent depuis l'étranger et dissimulent leurs traces en un tournemain. Inversement, la poursuite pénale se heurte constamment à des limites, de nature spatiale, au niveau du personnel et sous l'angle des moyens juridiques. Les connaissances particulières et les indispensables instruments techniques d'investigation manquent parfois. Immensité et confinement se font face, brutalement. Les appels hâtifs de la politique en faveur d'une efficacité accrue n'apportent rien. Des investissements, surtout, sont requis. Il faut dépenser de l'argent qui, plus tard, manquera peut-être ailleurs. Pareilles redistributions se font rarement sans accrocs. En outre, les corps de police et les ministères publics doivent renoncer à leur compétence en matière de cybercriminalité au profit de nouvelles régions – qui restent à définir – ou de la Confédération. Ici, on devrait bien finir par comprendre qu'un excès de responsabilité constituera tôt ou tard un fardeau paralysant.

Afin d'améliorer le savoir-faire des ministères publics, des tribunaux et de la police, l'Académie des procureurs offre dès 2019 une formation en cybercriminalité en trois phases. Le cycle débute par un enseignement de base sur la délinquance digitale quotidienne, celle qui engage l'informatique comme instrumentum sceleris *et moyen de preuve. Suivront un cours de droit pénal et de procédure pénale de la cybercriminalité, puis des leçons sur le crime high-tech à l'attention des meilleurs spécialistes des autorités pénales. Puissent les défenseurs au pénal mettre bientôt sur pied une formation similaire, car un procès gagne en qualité grâce à l'expertise de tous.*

Je vous souhaite de joyeuses fêtes de fin d'année.

Jürg-Beat Ackermann