WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION AMBA ACCREDITED

Rechtspanorama am 10. Juni 2024

Messenger-Dienste: Soll der Staat mitlesen?

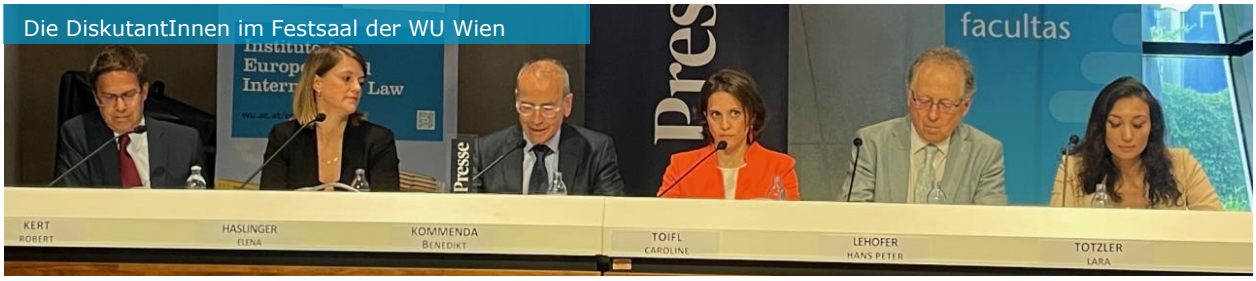
von *Moritz Anton Ibesich*

Vor dem Hintergrund der Aufhebung der bisherigen Regelungen zur Handysicherstellung und der regelmäßig aufkeimenden Diskussion um die Notwendigkeit, nicht nur gewöhnliche Telefonate und Textnachrichten, sondern auch solche, die über Ende-zu-Ende-verschlüsselte Messengerdienste übertragen werden, überwachen zu können, fand im Rahmen der traditionellen Veranstaltungsreihe „Rechtspanorama an der WU" eine Diskussionsveranstaltung zum Thema „Messenger-Dienste: Soll der Staat mitlesen" statt.

Vranes, Haslinger, Totzler, Lehofer, Toifl, Kert, Wittmann, Kommenda

Wer einer Telefonüberwachung entgehen will, kann auf WhatsApp, Telegram & Co. ausweichen. Soll der Staat bei solchen Messenger-Diensten online mitlesen dürfen? Unter welchen Voraussetzungen und zu welchem Zweck, zur Abwehr von Gefahren und/oder zur Aufklärung von Straftaten? Welche Grenzen setzen die Grundrechte und der Verfassungsgerichtshof? Zu diesen und weiteren brisanten Fragen bezogen folgende besonders ausgewiesene Diskutantinnen und Diskutanten im voll besetzten Festsaal 2 der WU Stellung:

1. **StA Mag. Elena Haslinger,** Präsidentin der Vereinigung österreichischer Staatsanwältinnen und Staatsanwälte
2. **Univ.-Prof. Dr. Robert Kert,** Vorstand des Instituts für Österreichisches und Europäisches Wirtschaftsstrafrecht an der WU Wien
3. **SP Hon.-Prof. Dr. Hans Peter Lehofer,** Senatspräsident des Verwaltungsgerichtshofes, Honorarprofessor an der WU Wien
4. **Dr. Caroline Toifl,** Rechtsanwältin und Steuerberaterin, C. Toifl Rechtsanwalt GmbH
5. **Lara Totzler, BA,** Senior Managerin bei Deloitte Wien im Bereich Cyber Risk



Die DiskutantInnen im Festsaal der WU Wien

Die Veranstaltung wurde in bewährter Manier am 10. Juni 2024 vom Institut für Europarecht und Internationales Recht der WU Wien gemeinsam mit der Tageszeitung „Die Presse" und mit freundlicher Unterstützung durch den „Facultas Verlag" organisiert. Moderiert wurde die Diskussion von ***Mag. Benedikt Kommenda***, Chef vom Dienst „Die Presse". ***Univ.Prof. Dr. Erich Vranes*, LL.M.**, Vorstand des Instituts für Europarecht und Internationales Recht der WU, hieß die Diskutantinnen und Diskutanten an der WU herzlich willkommen.

Zur Diskussion:

Die Ausgangslage

Die Aktualität der Thematik, die das Fundament der Diskussion darstellte, unterstrich der Moderator, *Benedikt Kommenda*, in seinen einleitenden Worten anhand der Widersprüchlichkeit zwischen den Überwachungsmöglichkeiten der Strafverfolgungsbehörden in Abhängigkeit der von vermeintlichen TäterInnen eingesetzten Kommunikationstechnologie. Während herkömmliche Kommunikationsmittel – wie SMS und Telefonate – nach richterlicher Genehmigung überwacht werden könnten, bestünde diese Möglichkeit bei der Kommunikation mittels Messengerdiensten nicht.

Kommenda

Unter welchen Voraussetzungen Kriminalpolizei und Staatsanwaltschaft hinkünftig Messangerdienste mitlesen dürfen sollen, sei die Kernfrage der gegenständlichen Veranstaltung, so der Moderator. Dabei sei eine wichtige Rechtsgüterabwägung, zwischen dem Interesse der Privatsphäre und der Verbrechensverhütung, durchzuführen und die technische Umsetzbarkeit nicht außer Acht zu lassen.

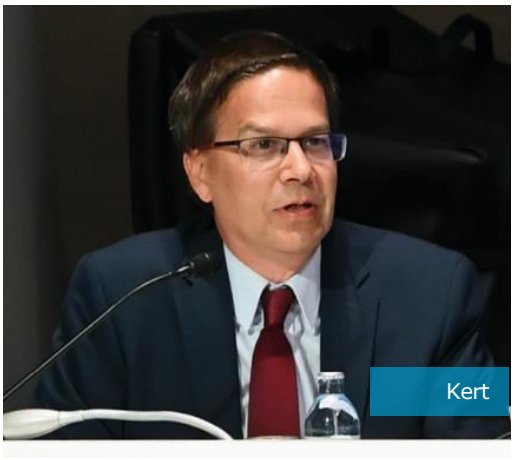
Der Blick der Strafverfolgungsbehörden


Haslinger

Elena Haslinger nahm zunächst eine Ist-Stand-Aufnahme vor und erläuterte, dass die Anpassung der rechtlichen an die technischen Möglichkeiten unabdingbar sei, um eine effektive Strafrechtspflege in der Gegenwart und Zukunft sicherzustellen.

Von besonderer Relevanz für die Verbrechensaufklärung sei die Kommunikationsüberwachung im Bereich der Suchtmitteldelikte und der staatsfeindlichen Vereinigungen. Zur Verhütung von Anschlägen wären die Staatsanwaltschaften derzeit auf ausländische Nachrichtendienste und deren Hinweise angewiesen. Dies verdeutliche den dringenden Handlungsbedarf, um souverän tätig sein zu können.

Die rechtswissenschaftliche Perspektive


Kert

Einen Einblick in die rechtlichen Anforderungen an eine Messengerüberwachung bot *Robert Kert*. Zunächst erläuterte er – bezugnehmend auf die Judikatur des VfGH zum sog Bundestrojaner –, dass bei einem solchen die Eingriffsintensität in das Recht auf Achtung des Privat- und Familienlebens besonders stark ausgeprägt sei. Dies liege daran, dass für die Installation einer Überwachungssoftware auf einem Handy oder Laptop physisch auf die Geräte zugegriffen werden müsse, um Sicherheitslücken auf dem Gerät bzw Programm auszunützen.

Vor dem Hintergrund der Vielzahl an Daten, die sich heutzutage auf Handys befinden, und der Tatsache, dass nicht nur Daten der Person, dessen Handy infiltriert wird, betroffen seien, sondern auch Daten von unbeteiligten Dritten, die lediglich mit der betroffenen Person in Kontakt standen, habe der VfGH den Bundestrojaner für unzulässig erachtet.

Eingriffe mit einer derart signifikanten Streuwirkung gegenüber unbetroffenen Dritten, die Rückschlüsse auf Gesinnungen, Neigungen und Lebensführung zulassen würden, bedürften zur Rechtfertigung schwerwiegender öffentlicher Interessen. Ein solches schwerwiegendes öffentliches Interesse wäre selbst bei der Beteiligung an einer terroristischen Vereinigung oder kriminellen Organisation, mit bis zu 10 Jahren Freiheitsstrafe bewährten Delikten, nicht gegeben, weil es sich bloß um qualifizierte Vermögensdelikte handle, führte der Vorstand des Instituts für Österreichisches und Europäisches Wirtschaftsstrafrecht an der WU Wien aus. Jedenfalls wäre eine begleitende, unabhängige richterliche Beaufsichtigung der Überwachungsmaßnahmen erforderlich.

Die technischen Rahmenbedingungen


Totzler

Die Fernüberwachung von Computersystemen, seien es Handys oder PCs erfordere *Softwarehintertüren bzw -lücken*, die ein Eindringen ermöglichen, erklärte *Lara Totzler*. Dafür könne bspw eine Spyware auf dem jeweiligen Gerät installiert werden, die die Kommunikation am Gerät selbst abfängt, noch bevor diese verschlüsselt werde. Eine bekannte Software für diesen Zweck sei

Pegasus, die noch nicht ausgemerzte Sicherheitslücken ausnütze und den Zugriff auf sämtliche Funktionen des infiltrierten Geräts erlaube, von der Kamera, über das Mikrofon, Text, den Bildschirm, usw. In der Vergangenheit sei diese Spyware von Nachrichtendiensten vielfach gegen JournalistInnen und MenschenrechtsaktivistInnen eingesetzt worden. Pegasus sei, so die Senior Managerin bei Deloitte Wien, in der Lage in Computersysteme einzudringen und diese zu kompromittieren, ohne dass der Nutzer mit einer Nachricht interagieren müsste, womit kein effektiver Schutz vor Angriffen möglich sei.

Die grundrechtliche Analyse


Lehofer

Einleitend bestätigte *Hans Peter Lehofer* die rechtliche Analyse von *Robert Kert* und legte dar, dass eine Überwachung in einer derart intensiven Form, wie es die Installierung einer Schadsoftware sei, nur unter äußerst engen Voraussetzungen möglich sei. Es bedürfe nicht nur einer unabhängigen Kontrolle derartiger Überwachungsmaßnahmen, sondern müssten überdies technisch geeignete Kontrollen der Observationen sichergestellt werden.

Der Honorarprofessor der WU Wien erläuterte, dass iS einer positiven Schutzpflicht des Staates die Aufklärung von Straftaten grundrechtlich geboten sein könne und dass es hierfür erforderlich wäre, Behörden mit ausreichenden Ressourcen auszustatten. Jedoch dürfe nicht übersehen werden, dass dies nicht in einem Vakuum geschehen könne, sondern jedenfalls eine Abwägung der entsprechenden Grundrechte erforderlich sei.

Der anwaltliche Blick


Toifl

Zu Beginn ihrer Ausführungen gab *Caroline Toifl zu bedenken*, dass die Tatsache, dass ein Ermittlungsverfahren geführt werde, noch nicht bedeute, dass jemand eine Straftat begangen habe, sondern lediglich, dass ein Verdacht bestünde. Die Rechtsanwältin führte aus, dass selbst das Erfordernis einer richterlichen Bewilligung ungenügend sei, weil es sich dabei um sog Stampiglienbeschlüsse handle, bei denen den Haft- und Rechtschutzrichter im Falle einer Bewilligung keine Begründungspflicht treffe, während die Ablehnung einer staatsanwaltlichen Anordnung sehr wohl einer Begründung bedürfe. Ergebnis dessen sei, dass lediglich eine von zweihundert Anordnungen nicht bewilligt werde. Zur Gewährleistung eines ausreichenden Rechtsschutzniveaus sei

eine inhaltliche Auseinandersetzung des Haft- und Rechtschutzrichters mit der Frage der konkreten Verhältnismäßigkeit unabdingbar.

Weiters müsse bei der Infiltration eines Endgerätes mittels eines Staatstrojaners sichergestellt werden, dass Daten nur bzgl bestimmter Taten und Zeiträume erhoben und ausgewertet werden dürfen. Die Erhebung und Auswertung der Daten solle überdies nicht durch die Staatsanwaltschaft bzw Kriminalpolizei erfolgen, sondern durch eine getrennte Stelle, die als Filter fungieren solle.

Zuletzt plädierte die Verteidigerin dafür, Beschuldigten iSd Waffengleichheit ein Einsichtsrecht in die aufgezeichneten Kommunikationsdaten zu gewähren, schließlich sei es nach mehreren Jahren mitunter nicht mehr möglich, sich an den Inhalt konkreter Gespräche zu erinnern.

Eine Novellierung der StPO sei zweifellos geboten, jedoch müsse ein ausreichendes Rechtsschutzniveau sichergestellt werden.

Die Präsidentin der Vereinigung österreichischer Staatsanwältinnen und Staatsanwälte replizierte bzgl der Kritik an den Stampiglienbewilligungen, die staatsanwaltlichen Anordnungen müssten ohnehin detailliert begründet werden und würde diese Begründung von Personen, namentlich StaatsanwältInnen, durchgeführt, die die gleiche Ausbildung absolviert hätten, wie die RichterInnen, die über diese entscheiden würden.
Robert Kert schloss sich dieser Kritik nicht an und gab zu bedenken, dass bei derart schwerwiegenden Eingriffen sogar überlegt werden sollte, einen Drei-Richter-Senat zu befassen.

Hinsichtlich eines Einsichtsrechts in die Überwachungsprotokolle für Beschuldigte führte *Hans Peter Lehofer* aus, dass dieses während der Observation nicht möglich sei, weil der Beschuldigte ansonsten wüsste, dass er überwacht wird und damit der Zweck der Überwachung vereitelt werden würde. Bei der Verwendung von Staatstrojanern sei es überdies ein großes Problem, sicherzustellen, dass die Software lediglich das überwachte Gerät an sich kompromittiert und die dort befindlichen Daten wahrheitsgemäß „spiegelt". Immerhin könne ex-post kaum kontrolliert werden, ob bspw die enthaltenen Zeitstempel korrekt seien, nachdem die Software – zumindest theoretisch – auch diese verändern könnte. Entscheidend sei es, sicherzustellen, dass die ausgelesenen Daten tatsächlich der Wirklichkeit entsprechen und nicht manipuliert wurden.

Auf die Ausführungen der PodiumsteilnehmerInnen folgte eine rege Diskussion, in die zahlreiche Fragen aus dem Publikum einflossen. Von der aktuellen Abhängigkeit von ausländischen Diensten, über die technische Begrenzbarkeit von Handyüberwachungen reichte die Diskussion bis zu den Anforderungen des VfGH an den Schutz von JournalistInnen und RechtsanwältInnen.