Strafbarkeitsrisiken bei E-Mail-Schutzmaßnahmen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Fallfrage

Zu betrachten war die Möglichkeiten einer Strafbarkeit, wenn E-Mails durch das zustellende System eines Arbeitgebers, einer Behörde oder einer Organisation z.B. einer Universität bearbeitet, abgefangen oder in anderer als normal üblicher Weise zugestellt werden um das System und den Empfänger vor Spam, Phishing und Viren zu schützen. In Frage kommt eine Strafbarkeit gem. § 206 StGB wegen Verletzung des Post- oder Fernmeldegeheimnisses, sowie gem. § 303a StGB wegen Datenveränderung.

Strafbarkeit gemäß § 206 StGB

Für eine Strafbarkeit gem. § 206 StGB wegen Verletzung des Post- oder Fernmeldegeheimnisses bedarf es immer Tatsachen, die durch das Post- oder Fernmeldegeheimnis geschützt sind. Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individualisierte Empfänger mit Hilfe des Telekommunikationsverkehrs (BVerfGE 115, 166 (182); 124, 43 (54). Nach der in der Literatur überwiegend vertreten Ansicht fallen auch E-Mails unter den Schutz des Fernmeldegeheimnisses (Kargl in Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Auflage 2017, Rn. 17; Altenhain in Münchener Kommentar zum StGB, 3. Auflage 2017 Rn. 32; Eisele in Schönke/Schröder Strafgesetzbuch, 30. Auflage 2019, Rn. 6b; Altvater in Leipziger Kommentar StGB, 12. Auflage 2009 Rn. 24). Jedoch wurde vom EuGH der Dienst G-Mail 2019 nicht als Telekommunikationsdienst eingestuft (C-193/18). Dies dürfte beispielhaft für die E-Mail als solche gelten. Gem. § 1 Abs. 1 S. 1 TMG würde die E-Mail damit als Telemedium eingestuft werden. Telemedien werden nach einer in der Literatur vertretenen Ansicht hingegen nicht vom Fernmeldegeheimnis geschützt (Eisele in Schönke/Schröder Strafgesetzbuch, 30. Auflage 2019, Rn. 6b; Kargl in Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Auflage 2017, Rn. 17). Somit dürfte die E-Mail nicht unter das Fernmeldegeheimnis fallen. Sich der Auffassung des EuGHs auch für die strafrechtliche Auslegung des Begriffes Telekommunikationsdienstleisters anzuschließen ist im Bereich des Internets vorzuziehen, da gerade in diesem Bereich aufgrund des grenzüberschreitenden Datenflusses insbesondere die Begriffsdefinitionen die Harmonisierung ermöglichen. (vgl. auch Nehlsen in Hildmann, Clouddienste im Hochschuleinsatz 2016/2017, S. 8).

Selbst wenn man davon ausgeht, dass der europarechtliche Begriff des Telekommunikationsdienstes ein engerer ist als der des deutschen Verfassungsrechtes ist in § 206 StGB trotzdem von dem europarechtlichen Begriff auszugehen. Das ist damit zu begründen, dass auch die Telekommunikationsdienstleister für verschiedene Tatbestände des § 206 StGB geeignete Täter sind. Wer Telekommunikationsdienstleister ist bestimmt sich nach § 3 TKG. Dieser ist europarechtskonform

Dienstort	Telefon und Fax	elektronische Post	Internet
Rechenzentrum c/o Universität Würzburg Am Hubland Z 8 97074 Würzburg	Telefon +49(0)931/31-84217 Telefax +49(0)931/31-84217-0	rz-stabsstelle-it-recht@uni-wuerzburg.de	https://www.rz.uni-wuerzburg.de/dienste/it-recht/

auszulegen und ist eben eine jener Normen, die der EuGH in seinem Urteil über E-Mails heranzog, demzufolge E-Mails keine Telekommunikation darstellen. Würde man für die Bestimmung des Schutzbereiches des Fernmeldegeheimnisses (die unkörperliche Übermittlung von Informationen an individualisierte Empfänger mit Hilfe des Telekommunikationsverkehrs) eine weitergehende verfassungsrechtliche Auslegung des Begriffes Telekommunikation zugrunde legen, aber bei der Bestimmung eines geeigneten Täters den europarechtlich auszulegenden Begriff aus dem TKG hätte man in einem Straftatbestand 2 verschiedene Definitionen für den Begriff Telekommunikation. Dies verstößt gegen das Bestimmtheitsprinzip.

Praxishinweis

In der Praxis bleibt fraglich, wie § 206 StGB tatsächlich angewendet wird, wenn in der gängigen Kommentarliteratur die E-Mail als vom Fernmeldegeheimnis erfasst aufgeführt wird. Es ist zu bezweifeln, dass tatsächlich jede Rechtsanwender:innen, egal ob Richter:in, Staatsanwält:in oder Anwält:in, den europarechtlichen Kontext sowie das EuGH-Urteil dabei im Hinterkopf hat, da es bei der Fülle an EuGH-Urteilen nahezu unmöglich ist alle zu kennen.

Strafbarkeit gemäß § 303a StGB

Strafbar gem. § 303a StGB wegen Datenveränderung macht sich wer rechtswidrig Daten (§ 202a Abs. 2 StGB) löscht, unterdrückt, unbrauchbar macht oder verändert. Wenn das E-Mail-Systems eines Arbeitgebers, einer Behörde oder einer Organisation z.B. einer Universität Veränderungen an E-Mails vornimmt ist bereits fraglich, ob dies überhaupt rechtswidrig ist, da die E-Mails als Daten eigentlich dieser über dem einzelnen Nutzer stehenden Struktur zu zuordnen sind. Es bleibt jedoch der jeweilige Einzelfall mit seinen individuellen Umständen zu beurteilen. Die organisationsweite E-Mail-Adresse wird aber in vielen Fällen der Erfüllungen von Geschäftszwecke oder gesetzlichen Aufgaben dienen und somit strafrechtlich auch bei persönlichen Mailboxen der Organisation als Gesamtheit zu zuordnen sein. Eine parallele Wertung zeigt auch das Zivilrecht bei der Anscheins- und Duldungsvollmacht. Darüber hinaus kommen je nach technischer und organisatorischer Ausgestaltung als weitere Rechtfertigungsgründe etwa aus Art. 32 DSGVO, §§ 13 Abs. 4 und 7 TMG und etwa für bayerische Behörden auch Art. 11 BayEGovG in Frage. In einigen Konstellation könnte auch § 100 TKG Eingriffe rechtfertigen.

Fazit

Organisationen werden nicht durch das Strafrecht an der jeweiligen Bedrohungslage angemessenen Schutzmaßnahmen für E-Mail-Systeme gehindert.

[1] Marie Hallung unterstützt die Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen, c/o Universität Würzburg, geleitet von Johannes Nehlsen.