Digital Society | ·Graben 17/10 | A-1010 Wien

per E-Mail an
team.s@bmj.gv.at
begutachtungsverfahren@parlament.gv.at

Digital Society
Graben 17/10
A-1010 Wien

+43 1 314 22 33-0
Info@DigiSociety.at

Wien, 12.05.2016

Betreff: Stellungnahme zum Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Staatsanwaltschaftsgesetz geändert werden (192/ME)

Sehr geehrte Damen und Herren,

Die Digitalisierung unserer Gesellschaft bringt umwälzende Veränderungen für die gesamte Gesellschaft, ob im privaten Umfeld oder für Unternehmen. Die Digital Society beschäftigt sich mit den Auswirkungen dieser Veränderungen auf die Gesellschaft, analysiert diese gemeinsam mit Experten und erarbeitet politische Lösungen für aktuelle gesellschaftliche Probleme.

Wir erlauben uns, im Sinne unserer Ziele im Folgenden zum Gesetzesentwurf Stellung zu nehmen.

Wir haben die in den Erläuterungen und im Gesetzestext festgehaltenen Vorgaben zur Überwachungssoftware – im Folgenden als "ÜSw" abgekürzt - analysiert und hinsichtlich ihrer logischen Konsistenz und besonders ihrer technischen Machbarkeit untersucht. Dabei fielen uns einige Inkonsistenzen zwischen den Erläuterungen und dem Gesetzestext aufgefallen, die im Folgenden ebenfalls dokumentiert werden.

Arbeitsgruppe

In den Erläuterungen wird in der Einleitung festgehalten, dass in den Jahren 2007/2008 eine interdisziplinäre Arbeitsgruppe eingesetzt war, die die Machbarkeit einer "Online-Durchsuchung" untersuchte. Die Erläuterungen halten fest, dass sich das technische Umfeld in der Zwischenzeit radikal weiterentwickelt hat, was auch unseren Einschätzungen entspricht. Es wäre daher sehr sinnvoll gewesen, wiederum eine solche Arbeitsgruppe einzuberufen, um diese Weiterentwicklungen in einem breiten Wissens- und Erfahrungsumfeld zu analysieren. Die nachfolgenden Analysen zeigen, dass bei der Ausarbeitung des Gesetzestextes mit einem recht begrenzten technischen Wissen vorgegangen wurde.

Installation via Fernzugriff

Während die Erläuterungen von "ausschließlich ... durch **direkte** Installation eines Überwachungsprogramms im Computersystem" sprechen findet sich eine solche Eingrenzung

nicht im Gesetzestext. Dort wird von "durch Installation eines Überwachungsprogramms im Computersystem" gesprochen, was auch eine Ferninstallation erlaubt.

§136a Abs 2 normiert unter Verwendung des Begriffs "unumgänglich", dass eine direkte Installation nur dann durchzuführen ist wenn andere, nicht näher genannte Methoden nicht erfolgreich sind. Allerdings bleibt neben einer direkten Installation technisch nur die Ferninstallation übrig, sodass im Gegenschluss der Gesetzestext die Ferninstallation als zu bevorzugende Installationsart der ÜSw normiert. Dies steht im Widerspruch zu den Erläuterungen, weswegen eine neuerliche Überarbeitung und Klarstellung empfohlen wird.

Geht man davon aus, dass eine Installation via Fernzugriff tatsächlich im Gesetz normiert werden soll, so ist unklar, wie eine Installation via Fernzugriff funktionieren soll. Alle Computersysteme müssen gegen unautorisierten Zugriff von aussen geschützt sein und sind es in der Regel auch. Eine Installation wäre dann nur mit Zustimmung einer Person möglich, die auf dem Computersystem über ausreichende Privilegien verfügt. Im Allgemeinen wird das die zu überwachende Person sein oder eine Person aus dem Nahfeld der zu überwachenden Person. Es ist daher unwahrscheinlich dass eine unentdeckte Installation möglich ist. Bleibt also nur die Installation über Schwachstellen im Computersystem. Es müsste also systematisch von aussen nach solchen Schwachstellen gesucht werden. Werden keine gefunden so besteht keine Möglichkeit einer Ferninstallation. Essenziell für die Bewertung der Effektivität einer Ferninstalltion ist also eine Analyse, wie hoch der Prozentsatz der Computersysteme ist, auf denen eine Schwachstelle zu finden ist. Ist dieser Prozentsatz niedrig so kann die ÜSw nur in wenigen Fällen eingesetzt werden. Die Wahrscheinlichkeit, dass eine Überwachung möglich ist und bei dieser Überwachung auch tatsächlich eine relevante Straftat aufgedeckt wird folgt einer hypergeometrischen Verteilung. Für eine aussagekräftige Analyse wäre daher zu erheben:

- Wie viele Verdächtige sind zu erwarten, bei denen ein genügender Anfangsverdacht für eine digitale Überwachung besteht?
- In wie vielen von diesen Verdächtigungsfällen werden tatsächlich terroristische Straftaten geplant, wie viele sind Fehlalarme?
- In wie vielen Fällen wird eine Überwachung auch tatsächlich möglich sein?

Für die ersten beiden Fragen sollten sich anhand von Statistiken historischer Fälle Basisdaten finden lassen, von denen extrapoliert werden kann. Daten für die dritte Frage können aus Statistiken von Virusverbreitungen bei Herstellern von Anti-Virus-Software erhoben werden, wobei hier nach Betriebssystemen bzw. Computersystemtypen zu unterscheiden ist.

Schon aus dieser kurzen Betrachtung erkennt man die Komplexität einer solchen Analyse. Es ist jedoch unabdingbar eine solche Analyse durchzuführen wenn man die Effizienz der digitalen Überwachung einschätzen und damit die Wirtschaftlichkeit der Maßnahme bewerten will.

Installation via Direktzugriff

Eine Installation via Direktzugriff bedeutet einen direkten physischen Zugang zum Computersystem. Während es bei PCs noch machbar erscheint, sich in Abwesenheit der zu überwachenden Person genügend lange Zugang zum PC zu verschaffen wird die Situation bei Laptops und besonders bei Smartphones deutlich schwieriger, da diese häufig von der zu überwachenden Person mitgeführt oder sogar im Falle der Smartphones kontinuierlich am Körper getragen werden. Eine unentdeckt bleibende Installation erscheint hier eher

unwahrscheinlich. Wird der Installationsversuch aber bemerkt so kann die zu überwachende Person ihr Verhalten entsprechend anpassen und über das überwachte Gerät keine kritische Kommunikation mehr führen, ja sogar absichtlich falsche Informationen einstreuen die die geplante Straftat erst möglich machen, indem Ablenkungsmanöver inszeniert werden.

Auch bei direktem Zugang zum überwachenden Gerät müssen Sicherheitsbarrieren überwunden werden. Es ist fraglich, ob bzw. bei welchen Geräten eine solche Überwindung möglich ist, ob diese Spuren hinterlässt, die zur Entdeckung der Überwachung führen und wie lange eine solche Installation auf dem jeweiligen Gerät dauert. All diese Fragen sind erst detailliert zu analysieren und eine Aussage über die mögliche Effizienz der Installationsmethoden zu treffen.

Verständigung aller durch die Überwachung betroffenen Personen

Nach §138 Abs 5 sollen alle von der digitalen Überwachung betroffenen Personen nachträglich von der Überwachungsmaßnahme informiert werden. Diese Bestimmung hat sich nicht geändert, sondern soll nur um die digitale Überwachung erweitert werden. Bisher galt diese Bestimmung für die Überwachung von Briefkorrespondenz sowie persönlicher Gespräche und Telefonate. Die Entwicklung in der digitalen Welt haben das Kommunikationsverhalten der Menschen stark verändert. Während man früher mit einigen dutzend Menschen regelmäßig kommunizierte hat sich die Anzahl der Kommunikationspartner in der digitalen Welt vervielfacht. Facebook-Accounts haben je nach Altersgruppe zwischen 100 und 600 Freunde, auf Twitter und Instagram liegen die Followerzahlen bei 100 bis 200. Es ist daher davon auszugehen, dass jede veröffentlichte Nachricht von mehreren hundert Personen gesehen werden kann. Jede dieser Personen ist potentiell von der Überwachung betroffen und daher zu verständigen.

In Online-Spielen interagieren Spieler mit einer nicht überschaubaren Anzahl an wechselnden Kommunikationspartnern und kommunizieren mit diesen über die in die Spiele eingebauten Chat-Funktionen schriftlich oder via Sprachchat. Auch wenn diese Interaktionen nur kurz und mitunter bruchstückhaft sind müssen sie dennoch überwacht und ausgewertet werden. Auch diese Personen sind von der Überwachung zu verständigen.

Soll diese Verständigung auf dem Postwege passieren so wäre für jede dieser vielen hundert Personen die exakte Identität zu erheben. Selbst wenn die Person ihren Echtnamen und nicht nur ein Pseudonym angegeben hat werden sich nur in den wenigsten Fällen genügend zusätzliche Daten wie Geburtsdatum ermitteln lassen die eine eindeutige Identifikation ermöglichen. Weiters wird sich ein guter Prozentsatz der Kontakte im Ausland befinden, bei denen eine einfache Identitätsermittlung über das österreichische Zentrale Melderegister nicht möglich ist.

Eine effektive Verständigung kann somit nur elektronisch unter Verwendung desselben Übertragungsmediums (Facebook, Twitter, Instagram, E-Mail, Online-Spiel etc.) erfolgen. Da es sich bei einer Überwachung um ein sehr sensibles Thema handelt hat die Verständigung unter größtmöglicher Wahrung der Privatsphäre zu erfolgen. Die Verständigung kann prinzipiell entweder über den Betreiber des Übertragungsmediums erfolgen oder über einen Account innerhalb des Übertragunsmediums.

Die Betreiber der Übertragungsmedien haben in praktisch keinem Fall einen Geschäftssitz innerhalb Österreichs und sind somit rechtlich für eine entsprechden Verständigung nicht verpflichtbar. Bleibt somit nur eine direkte Verständigung über einen Account.

Zum Schutz der Privatspähre darf mit den Betroffenen nur über private Chat-Möglichkeiten kommuniziert werden, um sie von der Überwachung zu informieren. Dies bedeutet, dass die überwachende Behörde in jedem der Kommunikationsmedien einen eigenen Account unterhalten müsste. Während dies in den herkömmlichen Social Media noch möglich erscheint wird es bei Online-Spielen schon problematischer, da diese für den Zugang teilweise monatliche Gebühren verlangen.

Weiters ist zu bedenken dass in Social Medien im Allgemeinen eine private Benachrichtigung nicht ohne weiters möglich ist, wenn die Kommunikationspartner nicht miteinander verbunden sind. Um in Twitter eine private Nachricht an eine Person versenden zu können muss diese Person dem Account der überwachenden Behörde folgen. Auf Facebook landen private Nachrichten von nicht verbundenen Accounts in einer eigenen Liste, von der viele gar nicht wissen dass sie existiert. Bei Online-Spielen ist eine private Chat-Nachricht oft nur möglich, wenn beide Accounts im Spiel eingeloggt sind. Andere Übertragungsmedien unterliegen ähnlichen Beschränkungen.

Aus all diesen Punkten wird klar, dass eine Benachrichtigung von einer digitalen Überwachung auf Grund der Gegebenheiten der digitalen Welt nicht im notwendigen Umfang oder nur unter exorbitantem Aufwand erfolgen kann, somit faktisch unmöglich ist. Da eine zuverlässige Benachrichtigung aber eine Grundvoraussetzung für den derzeitigen Gesetzesentwurf darstellt muss aus unserer Sicht gefordert werden den derzeitigen Entwurf zurück zu ziehen und erst nach Klärung der grundrechtlichen und technischen Problematik entsprechend geändert neu vorzulegen.

Protokollierung

Der Gesetzesentwurf sieht in §145 Abs 4 eine Protokollierung in einem Umfang vor, durch die jede nachträgliche Veränderung am Computersystem nachvollzogen werden können muss, und spricht in diesem Zusammenhang von Sicherungskopien.

Um jede Veränderung nachvollziehen zu können bedarf es eines Gesamtdatenabzugs des überwachten Computersystems. Ein solcher Gesamtdatenabzug würde die Möglichkeit einer Online-Durchsuchung bieten, welche jedoch nicht zulässig ist. Die Sicherungskopien sind daher entsprechend sicher zu verwahren, was jedoch nicht im Gesetz vermerkt ist.

Zu bedenken ist auch, dass zur Bewertung der Veränderungen am Computersystem die veränderten Daten betrachtet werden müssten, wobei nicht auszuschließen ist dass Daten verändert wurden, die nichts mit der der Überwachung zugrunde liegenden Verdächtigung zu tun haben und damit unter das Verbot der Online-Durchsuchung fallen. Dies erscheint grundrechtswidrig und muss daher detailliert analysiert werden.

Vielzahl der Systeme

Im Entwurf wird nur sehr bruchstückhaft aufgezählt, für welche Übertragungsmedien überhaupt eine ÜSw zu erstellen wäre. Konkret ist von WhatsApp, Skype, Dropbox und iCloud die Rede. Andere Social Media Services bzw. Kommunikationstechniken werden nicht erwähnt.

Aus unserer Sicht ergeben sich eine Vielzahl anderer digitaler Kommunikationsmethoden, deren Eigenheiten in die Überlegungen einfließen müssen. Die folgenden Services bieten einfache Möglichkeiten einer nicht-öffentlichen Kommunikation, wobei es sich nur um die in Europa gängigsten und bekanntesten handelt:

Facebook	Instagram	Threema
Facebook Messenger	IRC	Tumblr
FaceTime	Mumble	Twitter
Google Hangouts	Skype	Viber
Google Plus	Snapchat	Privates VoIP
ICQ	TeamSpeak	WhatsApp

Und last but not least E-Mail.

Jeder dieser Services verwendet ein anderes Übertragungsprotokoll, für das ein eigener Filter zu entwickeln ist. Weiters ist zu bedenken dass die zu überwachenden Endgeräte unterschiedliche Betriebssysteme aufweisen. Für PCs und Laptops müssen mindestens Windows und MacOS (eventuell Linux) unterstützt werden, für Tablets und Smartphones sind es Android, iOS und Windows. Die ÜSw muss auf all diesen Betriebssystemen laufen können, wobei auch noch Betriebssystemvarianten zu berücksichtigen sind. Windows wäre in Version 7, 8 und 10 zu unterstützen. MacOS gibt es in über zehn verschiedenen Varianten, ebenso Android, bei dem auch noch die unterschiedlichen Hardware-Architekturen ARM, MIPS, PPC und x86 zu berücksichtigen sind. iOS liegt ebenfalls in mehreren Varianten vor. Jede dieser Varianten weist subtile Eigenheiten auf, die eine Anpassung der ÜSw notwendig machen können. Im Lichte dieser Zahlen erscheint auch die Schätzung des initialen finanziellen Aufwandes für die Softwareentwickluing höchst fragwürdig und sollte unbedingt einer detaillierten Analyse unterzogen werden

Update-Problematik

Die Funktion der ÜSw besteht darin, Daten aus Applikationen abzugreifen, bevor diese ihre Kommunikationsdaten verschlüsseln. Dazu muss die ÜSw sich tief in die Applikationen einklinken, was in den meisten Fällen nicht ohne Änderung des Applikationsprogramms geht. Um sich wie in § 136a Abs 3 Z 2 funktionsunfähig zu machen oder sich zu deinstallieren bedeutet, dass sich die ÜSw aus den Applikationen entfernen und den ursprünglichen Zustand wiederherstellen können muss. Dazu muss die ÜSw eine Sicherungskopie der Applikationen angelegt haben. Fraglich ist, was passiert, wenn während der Überwachung vom Benutzer ein Update der überwachten Applikation eingespielt wird, denn dadurch wird die ursprüngliche Applikation überschrieben und damit auch die Eingriffspunkte der ÜSw in der Applikation. Die ÜSw müsste sich dann neuerlich in der Applikation installieren. Fraglich ist, ob sie das tun könnte, da sich möglicherweise die Eingriffspunkte geändert haben. Wahrscheinlich müsste die ÜSw ebenfalls einem Update unterzogen werden, damit sie wieder funktionsfähig ist. Das würde bedeuten dass eine Überwachung nur dann erfolgreich sein kann wenn die überwachten Applikationen nicht vom Überwachten einem Update unterzogen werden oder die ÜSw so

zeitnah mit einem parallelen Update versorgt wird dass es zu keiner wesentlichen Unterbrechung der Überwachung kommt.

Nimmt man die im vorigen Abschnitt dargestellte Vielzahl an zu überwachenden Applikationen her so wird deutlich, dass die ÜSw laufend mit hohem Aufwand aktuell gehalten werden muss um wirksam eingesetzt werden zu können. Auch dieser Punkt ist bei einer Analyse der Effektivität zu beachten.

Finanzielles

In der Wirkungsorientierten Folgenabschätzung (WFA) werden die Kosten ohne nähere Erläuterungen mit 550k€ für das erste Jahr und 450k€ für die folgenden Jahre beziffert ohne auch nur irgendwie darauf einzugehen, wie diese Zahlen zustande kommen. In der detaillierten Darstellung ist von Anschaffungskosten für Software im ersten Jahr und Lizenzkosten in den Folgejahren die Rede. Es werden keine Hardwarekosten erwähnt.

Aus den Erläuterungen ergibt sich dass die ÜSw die erhobenen Daten online an die Ermittlungsbehörden übertragen soll. Dies bedeutet, dass durch die Ermittlungsbehörden ein oder mehrere Server zu betreiben sind. Weiters sieht der Gesetzesvorschlag vor dass die Daten mit höchstmöglichem Schutz zu speichern sind um die Privatsphären der Betroffenen zu schützen. Auch dies erfordert zusätzliche Ressourcen. All diese Ressourcen sind nicht unerheblich und daher zu analysieren.

Dem Begriff „Lizenzgebühren“ ist zu entnehmen dass hier offenbar geplant ist Software zuzukaufen. Es stellt sich die Frage, warum ein so sensibles Softwareprodukt nicht selbst entwickelt wird, sodass keine Lizenzgebühren anfallen und – was noch weitaus wichtiger ist – man die volle Kontrolle über die ÜSw behält. Es ist an dieser Stelle festzuhalten dass aus Sicherheitssicht ein Auditieren der ÜSw unabdingbar ist um das ordnungsgemäße Funktionieren sicherstellen und die Existenz von Hintertüren in der Software ausschließen zu können. Sollte dem BMI ein konkretes Angebot vorliegen so muss dieses auf breiter Basis durch Experten analysiert werden. Die Nicht-Erwähnung von Hardware zur Datensammlung erweckt den Verdacht, dass die komplette Datensammlung und Datenspeicherung an eine externe Firma ausgelagert werden soll. Dies ist aus grund- und datenschutzrechtlichen Überlegungen höchst problematisch.

Fazit

Aus all den obenstehenden aufgeworfenen Fragen kann nur der Schluss gezogen werden dass keine auch nur annähernd ausreichende Analyse der Probleme einer ÜSw durchgeführt wurde. Die aufgelisteten Problempunkte zeigen deutlich, wie komplex die Thematik ist und wie viel Klärungsbedarf besteht.

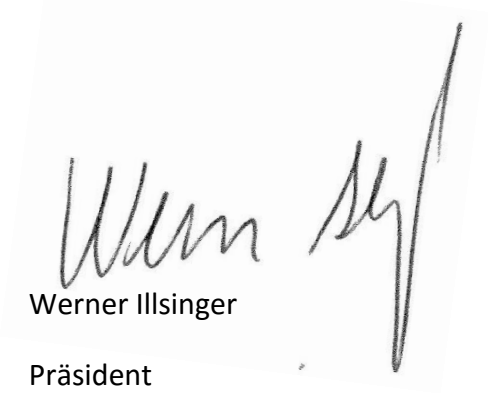
Aus unserer Sicht muss der vorliegende Gesetzesentwurf zurückgezogen und erst eine detaillierte Analsye der technischen Gegebenheiten, der Machbarkeit und letztlich der Effizienz der geplanten ÜSw durchgeführt werden. Eine solche Analyse ist nur im Rahmen einer interdisziplinären Arbeitsgruppe mit Teilnehmern mit sehr breit gefächertem Know-How möglich. Als Resultat ist ein technisch detailliertes Konzept inklusive Kostenschätzung vorzulegen, das einer öffentlichen Begutachtung zu unterziehen ist. Erst wenn sich das Konzept als machbar und finanziell akzeptabel erweist kann an eine juristische Umsetzung gedacht werden.

Wir hoffen, mit diesen Kommentaren einen wertvollen Beitrag geliefert zu haben und stehen für Rückfragen gerne zur Verfügung.

Mit freundlichen Grüßen,

Roland Giersig

Vizepräsident
Digital Society



Werner Illsinger

Präsident
Digital Society