4156/J
vom 16.11.2020 (XXVII. GP)

Anfrage

der Abgeordneten Dr. Harald Troch, Genossinnen und Genossen an die Bundesministerin für Justiz betreffend der Resolution 12143/1/20 des EU-Ministerrats.

Dem Österreichischen Rundfunk (ORF) liegt die Resolution 12143/1/20 REV 1 des EU-Ministerrats vor, in welchem die JustizministerInnen der EU beschlossen haben, den Datenschutz der EU-BürgerInnen (Art 8 EU-Grundrechtscharta), sowie das Recht auf das Privat- und Familienleben und die Kommunikationsfreiheit (Art 8 EMRK und Art 7 EU-Grundrechtscharta) erheblich zu beschneiden. Obwohl in dem Dokument eingangs die Wichtigkeit des Datenschutzes betont wird, kommen zahlreiche Medien zu dem Schluss, dass die Resolution dazu dient Messanger Apps und andere Online Plattformen zu zwingen, einen Zweit-Schlüssel ihrer E2E Verschlüsselung an Behörden abzutreten. Ein solcher Zugang zu den privatesten Nachrichten der EU-BürgerInnen könnte zukünftig leicht von Behörden und Personen, die Sicherheitslücken rund um den Zweit-Schlüssel ausnützen, missbraucht werden.

Anfrage

1. Eine Mehrheit der österreichischen Parteien sieht einen unmittelbaren und engen Zusammenhang zwischen den Grund- und Menschenrechten und einem zeitgemäßen Datenschutzes, wie in deren Grundsatzprogrammen dokumentiert ist. Die SPÖ fordert etwa:

   „Wir setzen uns für einen modernen und selbstbestimmten Datenschutz ein. Der Schutz der Privatsphäre ist wichtiger als wirtschaftliche Interessen. Der gläserne Bürger ist eine Gefahr für die Freiheit, weshalb wir für einen starken, einheitlichen und konsequent sanktionierten europäischen Datenschutz und einen digitalen Grundrechtskatalog eintreten"

   Im Programm der Grünen wird festgehalten:

   „In der weiteren Grundrechtsentwicklung wurde zwar teilweise den rapid zunehmenden Gefahren technischer Überwachungs- und Kontrollmechanismen Rechnung getragen (Datenschutz), im Großen und Ganzen ist jedoch vor allem im letzten Jahrzehnt ein Erosionsprozess der Grundrechte festzustellen: militärisch-polizeiliche Apparate haben gefährlich weit reichende Spitzelbefugnisse erhalten, wobei die international organisierte Kriminalität als Vorwand herhalten muss, um politische Andersdenkende und aktive BürgerInnen und deren Initiativen zu observieren.".

   Diese Positionen stehen auch im Einklang mit dem Rechten auf Datenschutz und Kommunikationsfreiheit, die die UN-Grundrechtecharta, allen BürgerInnen der Europäischen Union garantiert. Die Resolution des EU-Ministerrates steht im klaren Widerspruch zu diesen parteiprogrammatischen, menschenrechtlichen Forderungen. Haben Sie daher gegen die Resolution Einspruch erhoben, um die Menschen- und Bürgerrechte der ÖsterreicherInnen zu schützen?

2. Laut mehreren Berichten soll im Rat bereits Einstimmigkeit zu der Resolution bestehen. Dies würde jedoch bedeuten, dass Sie die Resolution unterstützen. Falls Sie der Resolution

tatsächlich zustimmen (würden), in welchem Ausmaß sind Sie bereit Grund- und Menschenrechte der österreichischen Bevölkerung aufzugeben und weshalb?

3. Besteht die Möglichkeit, dass im Rat die qualifizierte Mehrheit dennoch nicht erreicht wird, um diese Resolution zu beschließen und welche Schritten setzen Sie persönlich, um die qualifizierte Mehrheit zu verhindern?

4. Die feigen Terrorangriffe der letzten Wochen in Frankreich und Wien werden missbraucht, um im Eilverfahren diese Resolution vorbei an Zivilgesellschaft und nationalen Parlamenten durchzupressen. Welche sachliche Rechtfertigung haben Sie eine derartige Intransparenz in einem Rechtssetzungsprozess zu nutzen, in dem Grundrechte der BürgerInnen Österreichs und der Europäischen Union beschränkt werden sollen?

5. Nach den bisher bekannten Details, spielte Verschlüsselung keine entscheidende Rolle bei dem Attentat in Wien. Die schrecklichen Ereignisse in Wien geschahen, obwohl der Attentäter Polizei und Justiz bekannt war und obwohl klare Indizien (versuchter Munitionskauf) den Behörden alle Möglichkeiten gegeben hätten den Attentäter zu stoppen – auch ohne Zugriff auf seine Chatverläufe. Ist es für Sie vertretbar die Toten der Anschläge in Frankreich und Wien in einer solchen Weise für politische Zwecke zu missbrauchen, während eklatante Missstände bei den österreichischen Behörden existieren und diese daher nicht mehr die Sicherheit aller österreichischen BürgerInnen garantieren können?

6. Wie können österreichische Behörden nach solchen Verfehlungen, sowie nach jenen Verfehlungen, die den Gegenstand des BVT-Untersuchungsausschuss bilden, garantieren, dass sie mit den von ihnen gesammelten Daten der BürgerInnen sorgfältig umgehen und diese sicher und unzugänglich speichern?

7. Können Sie garantieren, dass die von den Behörden gesammelten Daten nicht für politische Motive missbraucht werden? Welche strafrechtlichen oder anderen Sanktionen sind für die handelnden Beamten, sowie für die politisch verantwortlichen Vertreter der Regierungsparteien vorgesehen, wenn es dennoch zu Verstößen kommt?

8. Anfang Dezember wird in einer weiteren Sitzung des Rates der Beschluss weiter behandelt und ggf. der Kommission der Auftrag erteilt, einen Entwurf für eine Verordnung zu entwerfen. Gedenken Sie – in Einklang mit oben genannten menschenrechtlichen Positionen – sich doch noch gegen diese Resolution auszusprechen, um ihre Umsetzung und damit den Beschnitt der Bürger- und Menschenrechte der EU-BürgerInnen zu verhindern?

9. Über die technische Umsetzung dieser Maßnahmen sind noch keine Details bekannt, allerdings wird in mehreren Berichten darüber gesprochen, dass Dienstbetreiber dazu gezwungen werden sollen, Hintertüren in ihre Software bzw. Verschlüsselung einzubauen. Im IT-Umfeld spricht man von einem sogenannten „Backdoor“. Sollte sich dies bewahrheiten, stellt dies eine erhebliche Sicherheitslücke für alle NutzerInnen dar, denn wie kann sichergestellt werden, dass die Kenntnis über diese Hintertüre nicht auch von Kriminellen-Netzwerken oder gar Terroristen selbst ausgenutzt wird?

10. Unter welchen Umständen sollen Behörden diese technische Hintertür ausnutzen dürfen? Muss dazu ein konkreter unmittelbarer Verdacht für eine schwere Straftat bestehen?

11. Muss eine unabhängige Stelle solch einen Zugriff genehmigen?

    11.1. Falls ja, welche Behörde soll dies sein?

    11.2. Falls nein, wem obliegt die Kontrolle eines solchen Einschnitts in die Privatsphäre der EU-BürgerInnen?

12. In mehreren Berichten ist ebenfalls zu lesen, dass sogenannte „Generalschlüssel" zum Aufbrechen der Messenger-Verschlüsselung auf IT-Systemen von Behörden hinterlegt werden sollen. Sollte dies technisch überhaupt machbar sein, wie kann der Missbrauch oder gar Verlust dieser Schlüssel sichergestellt werden?

13. Handelt es sich bei diesen „Generalschlüssel" nicht um ein selbst generiertes Angriffsziel, das in den falschen Händen enormen Schaden anrichten kann?

14. Der Generalschlüssel erinnert an das Vorgehen mit dem „Bundestrojaner", welcher vom VfGH als nicht verfassungskonform abgelehnt wurde. Können Sie erklären wie sich dieser geplante „Generalschlüssel" vom Bundestrojaner unterscheidet? Denken Sie, dass dieser nicht auch vom österreichischen VfGH abgelehnt wird?

15. Werden Bürgerinnen und Bürger nachträglich darüber informiert, wenn ihre privaten Nachrichten mitgelesen wurden und der Verdacht sich nicht erhärtet hat?

16. In der Resolution ist von „competent authorities" die Rede. Insbesondere französische und britische Geheimdienste pochen seit Jahren darauf, dass Messenger-Dienste „Backdoors" in ihre Dienste einbauen. Zählen daher auch Geheimdienste zu den „competent authorities"?

    Falls ja:

    16.1. Wem wird die Kontrolle der Geheimdienste obliegen?

    16.2. Unter welchen Umständen und mit wessen Genehmigung werden Geheimdienste das Recht erhalten auf die Daten österreichischer BürgerInnen zuzugreifen?

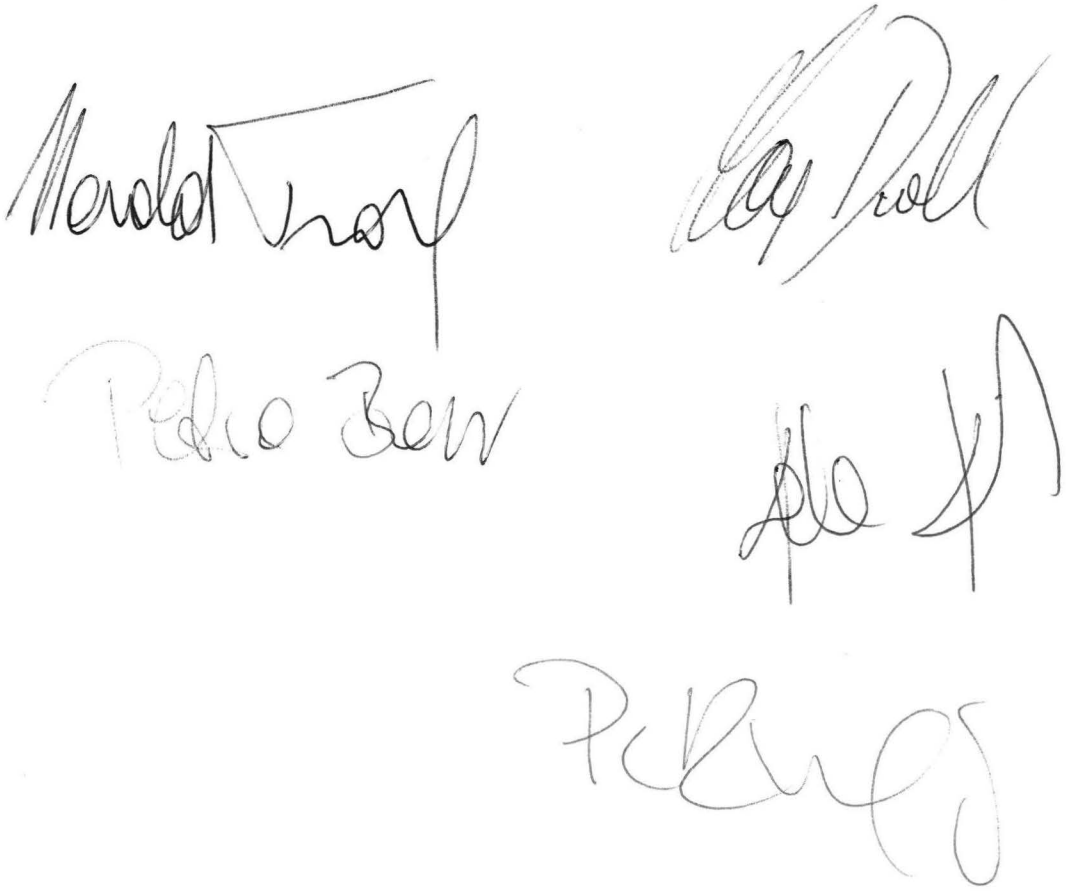
    16.3. Wird jeder Staat einen eigenen „Schlüssel" erhalten oder werden, beispielsweise, französische Geheimdienste die Möglichkeit haben, mit dem gleichen Schlüssel auf die Chats und Daten österreichischer BürgerInnen zuzugreifen?

17. Sollten europäische Geheimdienste Zugang erhalten, wie kann sichergestellt werden, dass sensible Daten österreichischer BürgerInnen nicht an andere Staaten weitergebeben werden?

17.1. Im Rahmen der Zusammenarbeit der EU-27 ist es Praxis, dass Geheimdienste ihre Informationen austauschen. Können Sie jedenfalls ausschließen, dass Daten österreichischer BürgerInnen nicht an Staaten außerhalb der EU-27 weitergegeben werden?

17.1.1. Falls ja, wie kann dies bewerkstelligt werden?

17.1.2. Falls nein, wieso nicht und was gedenken Sie dagegen zu unternehmen?



REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-11-16T15:23:03+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	