Raad van de
Europese Unie



Brussel, 24 november 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

**NOTA**

| | |
|---|---|
| van: | het voorzitterschap |
| aan: | de delegaties |
| nr. vorig doc.: | 12863/20 |
| Betreft: | Resolutie van de Raad over versleuteling<br>- Beveiliging dankzij versleuteling en beveiliging ondanks versleuteling |

Voor de delegaties gaat hierbij de resolutie van de Raad over versleuteling.

**Resolutie van de Raad over versleuteling**
**Beveiliging dankzij versleuteling en beveiliging ondanks versleuteling**

1. Preambule: beveiliging dankzij versleuteling en beveiliging ondanks versleuteling

De Europese Unie staat volledig achter de ontwikkeling, invoering en toepassing van krachtige versleuteling. De Europese Unie onderstreept dat de volledige naleving van de grondrechten, de mensenrechten en de rechtsstaat moet worden gewaarborgd bij alle acties in verband met deze resolutie, zowel online als offline. Versleuteling is noodzakelijk voor het beschermen van de grondrechten en de digitale beveiliging van overheden, het bedrijfsleven en de samenleving. Tegelijkertijd moet de Europese Unie ervoor zorgen dat de voor beveiliging en het strafrecht bevoegde instanties, zoals de rechtshandhavings- en justitiële autoriteiten, hun wettelijke bevoegdheden zowel online als offline kunnen uitoefenen om onze samenleving en burgers te beschermen.

Volgens de conclusies van de Europese Raad van 1-2 oktober 2020 (EUCO 13/20) *zal de EU haar instrumenten en regelgevende bevoegdheden ten volle inzetten om mondiale regels en normen te helpen vormgeven*. Er is overeengekomen dat middelen van de faciliteit voor herstel en veerkracht zullen worden ingezet ter verwezenlijking van doelstellingen als *het versterken van het vermogen van de EU om zichzelf te beschermen tegen cyberdreigingen, om een beveiligde communicatieomgeving te verschaffen, met name via kwantumencryptie, en om toegang tot data voor justitiële en rechtshandhavingsdoeleinden te waarborgen*.

2. Huidig gebruik/stand van versleuteling

Versleutelingstechnologie wordt tegenwoordig steeds meer voor alle mogelijke publieke en particuliere toepassingen gebruikt. Het is een middel om individuen, het maatschappelijk middenveld, kritieke infrastructuur, media en journalisten, het bedrijfsleven en overheden te beschermen door de privacy, vertrouwelijkheid, gegevensintegriteit en beschikbaarheid van communicatie en persoonsgegevens te waarborgen, en het is dus zonneklaar dat iedereen baat heeft bij versleutelingstechnologie. EU-gegevensbeschermings- en cyberbeveiligingsinstanties hebben te kennen gegeven dat versleuteling een belangrijk instrument is voor bijvoorbeeld de bescherming van persoonsgegevens die worden doorgegeven buiten de EU maar waarvoor een in wezen gelijkwaardig beschermingsniveau geldt, volgens het Hof van Justitie een wettelijke vereiste voor gegevensdoorgifte[1]. Niet alleen worden steeds meer elektronische apparaten en toepassingen dusdanig geprogrammeerd dat opgeslagen gebruikersgegevens standaard versleuteld worden, maar ook steeds meer communicatiekanalen en gegevensopslagdiensten worden met eind-tot-eindversleuteling (E2E) beveiligd. De positieve weerslag daarvan is terug te zien in de sterkere respons van de communicatie- en softwareapplicatiesector waar de meeste apps voor instant messaging en andere onlineplatforms tegenwoordig ook eind-tot-eindversleuteling gebruiken.

3. Uitdagingen bij het waarborgen van de beveiliging

Het "digitale leven" en de cyberruimte bieden niet alleen grote kansen, maar houden ook aanzienlijke uitdagingen in: de digitalisering van moderne samenlevingen brengt bepaalde kwetsbaarheden en mogelijk misbruik voor criminele doeleinden met zich mee. Criminelen kunnen zo overal verkrijgbare, kant-en-klare versleutelingsoplossingen inzetten die voor legitieme doeleinden zijn ontworpen[2].

Tegelijkertijd is de wetshandhaving steeds afhankelijker van toegang tot elektronisch bewijsmateriaal om terrorisme, georganiseerde misdaad, seksueel misbruik van kinderen (met name de online-aspecten daarvan) en een verscheidenheid aan andere cybercriminaliteit en cybermisdrijven doeltreffend te kunnen bestrijden. Het kan voor bevoegde instanties essentieel zijn dat zij toegang tot elektronisch bewijsmateriaal hebben, niet alleen voor een succesvolle opsporing en dus berechting van criminelen, maar ook om slachtoffers te beschermen en mee voor beveiliging te zorgen.

---

1 Arrest van 16 juli 2020 in zaak C-311/18, Data Protection Commissioner/Facebook Ireland Ltd en Maximillian Schrems, ECLI:EU:C:2020:559:.

2 iOCTA 2020, blz. 25.

In sommige gevallen echter is het als gevolg van versleuteling uiterst moeilijk of zelfs praktisch onmogelijk om toegang te krijgen tot, en de inhoud te analyseren van communicaties in het kader van de toegang tot elektronisch bewijsmateriaal, ook al is die toegang als zodanig rechtmatig. Het is daarom cruciaal ervoor te zorgen dat de voor beveiliging en het strafrecht bevoegde instanties, ongeacht de stand der technologie op een gegeven tijdstip, door middel van rechtmatige toegang hun bevoegdheden behouden om hun wettelijk voorgeschreven en toegestane taken uit te voeren. Dergelijke wetgeving waarin de handhavingsbevoegdheden worden geregeld, moet te allen tijde de eerlijke rechtsbedeling en andere waarborgen, alsmede de grondrechten in acht nemen, met name het recht op eerbiediging van het privéleven en communicatie en het recht op bescherming van persoonsgegevens.

4. Een juist evenwicht vinden

Het beginsel van beveiliging dankzij versleuteling en beveiliging ondanks versleuteling moet integraal worden hooggehouden. De Europese Unie blijft voorstander van krachtige versleuteling. Versleuteling biedt houvast voor het vertrouwen in het digitale domein en in de bescherming van de grondrechten, en moet daarom worden gestimuleerd en ontwikkeld.

Het is extreem belangrijk dat de privacy en de beveiliging van communicatie worden beschermd door middel van versleuteling en dat er tegelijkertijd voor wordt gezorgd dat de voor beveiliging en het strafrecht bevoegde instanties zich rechtmatig toegang tot relevante gegevens kunnen blijven verschaffen voor legitieme, duidelijk omschreven doeleinden bij de bestrijding van ernstige en/of georganiseerde criminaliteit en terrorisme - ook in de digitale wereld - en de handhaving van de rechtsstaat. Bij alle ondernomen acties moeten deze belangen zorgvuldig worden afgewogen tegen de beginselen van noodzakelijkheid, evenredigheid en subsidiariteit.

5. De krachten bundelen met de technologiesector

De Europese Unie streeft met de blik op de toekomst naar een actieve discussie met de technologiesector waarbij ook de onderzoeks- en academische wereld wordt betrokken, opdat ook verder krachtige versleutelingstechnologie wordt ingevoerd en toegepast. De bevoegde autoriteiten moeten zich, met volledige inachtneming van de grondrechten en de toepasselijke gegevensbeschermingswetgeving, op rechtmatige en doelgerichte wijze toegang tot gegevens kunnen verschaffen en tegelijkertijd de cyberbeveiliging kunnen garanderen. Technische oplossingen voor toegang tot versleutelde gegevens moeten voldoen aan de beginselen van wettigheid, transparantie, noodzakelijkheid en evenredigheid, met inbegrip van de bescherming van persoonsgegevens door ontwerp en door standaardinstellingen.

Aangezien er meerdere manieren zijn om de doelstellingen te bereiken, moeten overheden, het bedrijfsleven, de onderzoekswereld en de academische wereld op transparante wijze samenwerken om dit evenwicht strategisch tot stand te brengen.

6. Regelgevingskader

Er kan nader bekeken worden of er een EU-breed regelgevingskader moet worden ontwikkeld waarmee bevoegde instanties hun operationele taken doeltreffend kunnen uitvoeren en tegelijkertijd de privacy, de grondrechten en de beveiliging van de communicatie worden beschermd.

Potentiële technische oplossingen moeten overheden de mogelijkheid bieden hun onderzoeksbevoegdheden uit te oefenen, die krachtens hun nationale wetgeving onderworpen zijn aan evenredigheid, noodzakelijkheid en gerechtelijk toezicht, en daarbij gemeenschappelijke Europese waarden in acht te nemen, de grondrechten te eerbiedigen, en de voordelen van versleuteling te behouden. Mogelijke oplossingen moeten ontwikkeld worden op een transparante manier en in samenwerking met nationale en internationale aanbieders van communicatiediensten en andere relevante belanghebbenden. Voor deze technische oplossingen en normen - en een snelle technologische ontwikkeling in het algemeen - is tevens een voortdurende verbetering nodig van de technische en operationele vaardigheden en deskundigheid van de bevoegde instanties om de uitdagingen van de digitalisering op hun werkterrein op wereldschaal doeltreffend aan te pakken.

7. Innovatieve opsporingscapaciteiten

Ten slotte is het van het allergrootste belang de coördinatie op EU-niveau te verbeteren, teneinde:

1) de inspanningen van alle lidstaten en alle EU-instellingen en -organen te bundelen;

2) innovatieve wijzen van aanpak met het oog op nieuwe technologieën te definiëren en in te voeren;

3) passende technische en operationele oplossingen te analyseren; en

4) op maat gesneden hoogwaardige opleidingen aan te bieden.

Er zijn technische en operationele oplossingen nodig die verankerd zijn in een regelgevingskader dat gebaseerd is op de beginselen van wettigheid, noodzakelijkheid en evenredigheid. Die oplossingen moeten worden ontwikkeld in nauw overleg met dienstverleners, andere relevante belanghebbenden en alle relevante bevoegde instanties, waarbij moet worden aangetekend dat niet noodzakelijkerwijs moet worden gestreefd naar een enkele voorgeschreven technische oplossing voor toegang tot versleutelde gegevens.