Съвет на
Европейския съюз

Брюксел, 24 ноември 2020 г.
(OR. en)

13084/1/20
REV 1

LIMITE

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

БЕЛЕЖКА

От:	Председателството
До:	Делегациите
№ предх. док.:	12863/20
Относно:	Резолюция на Съвета относно криптирането – Сигурност чрез криптиране и въпреки него

Приложено на делегациите се изпраща резолюцията на Съвета относно криптирането.

ПРИЛОЖЕНИЕ

Резолюция на Съвета относно криптирането
Сигурност чрез криптиране и въпреки него

1. Увод: Сигурност чрез криптиране и въпреки него

Европейският съюз напълно подкрепя разработването, прилагането и използването на стабилно криптиране. Европейският съюз подчертава необходимостта да се гарантира пълно зачитане на основните права, правата на човека и върховенството на закона във всички действия, свързани с настоящата резолюция, както онлайн, така и офлайн. Криптирането е необходимо средство за защита на основните права и цифровата сигурност на правителствата, промишлеността и обществото. Същевременно Европейският съюз трябва да гарантира, че компетентните органи в областта на сигурността и наказателното правосъдие, например правоприлагащите и съдебните органи, могат да упражняват своите законни правомощия – както онлайн, така и офлайн, за да защитават нашите общества и граждани.

Според заключенията на Европейския съвет от 1 – 2 октомври 2020 г. (EUCO 13/20) *ЕС ще използва инструментите и регулаторните си правомощия, за да помогне за оформянето на глобалните правила и стандарти*. Изразено беше съгласие, че средствата по линия на Механизма за възстановяване и устойчивост ще се използват за постигане на цели като *повишаване на способността на ЕС за защита срещу киберзаплахи, за предоставяне на сигурна комуникационна среда, по-специално чрез квантово криптиране, и за осигуряване на достъп до данни за целите на съдебните и правоприлагащите органи*.

2. Настоящо използване/състояние на криптирането

В днешния свят технологията за криптиране все повече се използва във всички области на обществения и личния живот. Това е средство за защита на физическите лица, гражданското общество, критичните инфраструктури, медиите и журналистите, промишлеността и правителствата чрез гарантиране на неприкосновеността на личния живот, поверителността, интегритета на данните и наличността на комуникациите и личните данни: безспорно е, че технологията за криптиране е полезна за всички страни. Криптирането беше определено от органите на ЕС за защита на данните и киберсигурност като важен инструмент, който допринася например за защитата на личните данни, предавани извън ЕС, при условие че се спазва изискването за равностойно по същество ниво на защита, което според Съда е правно изискване за предаването на данни[1]. Не само електронните устройства и приложения все повече се програмират за криптиране на съхраняваните данни на потребителите по подразбиране, но нараства и броят на каналите за комуникация и услуги за съхранение на данни, които също са защитени чрез криптиране от край до край (E2E). Нараства положителната реакция в отговор на това от страна на сектора на комуникациите и приложенията, където по-голямата част от приложенията за незабавни съобщения и други онлайн платформи също са въвели криптиране от край до край.

3. Предизвикателства пред гарантирането на сигурността

„Дигиталният живот“ и киберпространството създават не само големи възможности, но и значителни предизвикателства: цифровизацията на съвременните общества носи със себе си известни уязвимости и потенциал за използване с престъпни цели. По този начин в своите методи на действие престъпниците могат да включват леснодостъпни, готови решения за криптиране, разработени за законни цели[2].

В същото време правоприлагането е все по-зависимо от достъпа до електронни доказателства за ефективна борба с тероризма, организираната престъпност, сексуалното насилие над деца (особено неговите онлайн аспекти), както и с редица други киберпрестъпления и престъпления, извършвани благодарение на киберпространството. За компетентните органи достъпът до електронни доказателства може да бъде от съществено значение не само за провеждане на успешни разследвания и за изправяне на престъпниците пред съда, но и за защита на жертвите и за гарантиране на сигурността.

---

[1] Решение от 16 юли 2020 г. по дело C-311/18, Data Protection Commissioner срещу Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

[2] iOCTA 2020, стр. 25.

Има обаче случаи, в които криптирането прави достъпа до и анализа на съдържанието на комуникациите в рамките на достъпа до електронни доказателства изключително трудни или практически невъзможни, въпреки факта, че достъпът до такива данни би бил законен. Следователно, независимо от днешната технологична среда, от съществено значение е да се запазят правомощията на компетентните органи в областта на сигурността и наказателното правосъдие чрез законен достъп за изпълнение на техните задачи, както е предвидено и разрешено от закона. Такива закони, предвиждащи правомощия за правоприлагане, трябва винаги изцяло да зачитат правото на справедлив процес и другите гаранции, както и основните права, по-специално правото на зачитане на личния живот и комуникациите и правото на защита на личните данни.

4. Постигане на точния баланс

Принципът на сигурност чрез криптиране и въпреки него трябва да бъде спазван в своята цялост. Европейският съюз продължава да подкрепя стабилното криптиране. То лежи в основата на доверието в цифровизацията и в защитата на основните права и следва да бъде насърчавано и развивано.

От изключителна важност е да се защитава неприкосновеността на личния живот и сигурността на комуникациите чрез криптиране, като едновременно с това се утвърждава възможността за законен достъп на компетентните органи в областта на сигурността и наказателното правосъдие до съответните данни за законни и ясно определени цели в борбата с тежката и/или организираната престъпност и тероризма, включително в света на цифровите технологии, и като се зачита върховенството на закона. Всички предприети действия трябва внимателно да балансират тези интереси с принципите на необходимост, пропорционалност и субсидиарност.

5. Обединяване на усилията с технологичния сектор

По пътя си напред Европейският съюз се стреми към активна дискусия с технологичния сектор, привличайки към нея научноизследователските и академичните среди, за да се гарантира непрекъснатото прилагане и използване на стабилни технологии за криптиране. Компетентните органи трябва да имат достъп до данните по законен и целенасочен начин, при пълно зачитане на основните права и съответните закони за защита на данните, като същевременно утвърждават киберсигурността. Техническите решения за получаване на достъп до криптирани данни трябва да съответстват на принципите на законност, прозрачност, необходимост и пропорционалност, включително защита на личните данни още при проектирането и по подразбиране.

Тъй като не съществува един-единствен начин за постигане на поставените цели, правителствата, промишлеността, научноизследователските и академичните среди трябва да работят заедно по прозрачен начин, за да създадат този баланс по стратегически начин.

6. Регулаторна рамка

Може да бъде допълнително оценена необходимостта от разработване на регулаторна рамка в ЕС, която да позволи на компетентните органи да изпълняват ефективно оперативните си задачи, като същевременно защитават неприкосновеността на личния живот, основните права и сигурността на комуникациите.

Потенциалните технически решения ще трябва да позволят на органите да използват своите правомощия за разследване при спазване на принципите на пропорционалност, необходимост и съдебен контрол съгласно тяхното национално законодателство, като същевременно утвърждават общите европейски ценности и основните права и като запазват предимствата на криптирането. Възможните решения следва да се разработват по прозрачен начин в сътрудничество с националните и международните доставчици на комуникационни услуги и други заинтересовани страни. Тези технически решения и стандарти, както и бързото развитие на технологиите като цяло, ще изискват и непрекъснато подобряване на техническите и оперативните умения и експертния опит на компетентните органи с цел ефективно справяне с предизвикателствата на цифровизацията в работата им в световен мащаб.

7. Иновативни способности за разследване

И накрая, от първостепенно значение е да се подобри координацията на равнище ЕС, насочена към:

1) обединяване на усилията на всички държави членки и на институциите и органите на ЕС;

2) определяне и установяване на иновативни подходи с оглед на новите технологии;

3) анализиране на подходящи технически и оперативни решения; и

4) предоставяне на адаптирано висококачествено обучение.

Техническите и оперативните решения, заложени в регулаторна рамка, изградена върху принципите на законност, необходимост и пропорционалност, следва да бъдат разработени в тесни консултации с доставчиците на услуги, други съответни заинтересовани страни и всички имащи отношение компетентни органи, въпреки че не следва да има едно-единствено предписано техническо решение за предоставянето на достъп до криптирани данни.