Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 24 Νοεμβρίου 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

ΣΗΜΕΙΩΜΑ

Αποστολέας:	Προεδρία
Αποδέκτης:	Αντιπροσωπίες
αριθ. προηγ. εγγρ.:	12863/20
Θέμα:	Ψήφισμα του Συμβουλίου για την κρυπτογράφηση - Ασφάλεια μέσω κρυπτογράφησης και ασφάλεια παρά την κρυπτογράφηση

Διαβιβάζεται στις αντιπροσωπίες στο παράρτημα το ψήφισμα του Συμβουλίου για την κρυπτογράφηση.

ΠΑΡΑΡΤΗΜΑ

Ψήφισμα του Συμβουλίου σχετικά με την ασφάλεια μέσω κρυπτογράφησης και την ασφάλεια παρά την κρυπτογράφηση

1. Προοίμιο: Ασφάλεια μέσω κρυπτογράφησης και ασφάλεια παρά την κρυπτογράφηση

Η Ευρωπαϊκή Ένωση υποστηρίζει πλήρως την ανάπτυξη, την εφαρμογή και τη χρήση ισχυρής κρυπτογράφησης. Η Ευρωπαϊκή Ένωση υπογραμμίζει την ανάγκη να διασφαλιστεί ο πλήρης σεβασμός των θεμελιωδών και ανθρωπίνων δικαιωμάτων και του κράτους δικαίου σε κάθε ενέργεια που σχετίζεται με το παρόν ψήφισμα, τόσο εντός όσο και εκτός διαδικτύου. Η κρυπτογράφηση είναι απαραίτητο μέσο προστασίας των θεμελιωδών δικαιωμάτων και της ψηφιακής ασφάλειας των κυβερνήσεων, της βιομηχανίας και της κοινωνίας. Ταυτόχρονα, η Ευρωπαϊκή Ένωση πρέπει να διασφαλίσει την ικανότητα των αρμόδιων αρχών στον τομέα της ασφάλειας και της ποινικής δικαιοσύνης, π.χ. αρχών επιβολής του νόμου και δικαστικών αρχών, να ασκούν τις νόμιμες εξουσίες τους, τόσο εντός όσο και εκτός διαδικτύου, για την προστασία των κοινωνιών και των πολιτών μας.

Σύμφωνα με τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου της 1ης και 2 Οκτωβρίου 2020 (EUCO 13/20), *η ΕΕ θα αξιοποιήσει τα εργαλεία και τις κανονιστικές εξουσίες της για να συμβάλει στη διαμόρφωση παγκόσμιων κανόνων και προτύπων*. Συμφωνήθηκε ότι τα κονδύλια στο πλαίσιο του μηχανισμού ανάκαμψης και ανθεκτικότητας θα χρησιμοποιηθούν για την προώθηση στόχων όπως η *ενίσχυση της ικανότητας της ΕΕ να αυτοπροστατεύεται από απειλές στον κυβερνοχώρο, να παρέχει ασφαλές περιβάλλον επικοινωνίας, ιδίως μέσω κβαντικής κρυπτογράφησης, και να διασφαλίζει την πρόσβαση σε δεδομένα για δικαστικούς σκοπούς και για σκοπούς επιβολής του νόμου.*

2. Τρέχουσα χρήση/κατάσταση της κρυπτογράφησης

Στον σημερινό κόσμο, η τεχνολογία κρυπτογράφησης χρησιμοποιείται όλο και περισσότερο σε όλους τους τομείς της δημόσιας και της ιδιωτικής ζωής. Αποτελεί ένα μέσο για την προστασία των ατόμων, της κοινωνίας των πολιτών, των υποδομών ζωτικής σημασίας, των μέσων ενημέρωσης και των δημοσιογράφων, της βιομηχανίας και των κυβερνήσεων, διά της διασφάλισης της ιδιωτικότητας, της εμπιστευτικότητας, της ακεραιότητας δεδομένων και της διαθεσιμότητας των επικοινωνιών και των δεδομένων προσωπικού χαρακτήρα: είναι προφανές ότι όλοι οι εμπλεκόμενοι ωφελούνται από την τεχνολογία κρυπτογράφησης. Η κρυπτογράφηση έχει αναγνωριστεί από τις αρχές της ΕΕ για την προστασία των δεδομένων και την ασφάλεια στον κυβερνοχώρο ως σημαντικό εργαλείο που συμβάλλει, για παράδειγμα, στην προστασία δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται μεν εκτός ΕΕ αλλά υπό την προϋπόθεση της απαίτησης ουσιωδώς ισοδύναμου επιπέδου προστασίας, κάτι που, σύμφωνα με το Δικαστήριο της ΕΕ, αποτελεί νομική απαίτηση για τις διαβιβάσεις δεδομένων[1]. Δεν είναι μόνον οι ηλεκτρονικές συσκευές και εφαρμογές που προγραμματίζονται όλο και συχνότερα να κρυπτογραφούν εξ ορισμού τα αποθηκευμένα δεδομένα χρήστη, αλλά όλο και περισσότεροι δίαυλοι επικοινωνίας και υπηρεσίες αποθήκευσης δεδομένων προστατεύονται με διατερματική κρυπτογράφηση (E2E). Αυτό αντικατοπτρίζεται θετικά στην αυξανόμενη ανταπόκριση του κλάδου της επικοινωνίας και των εφαρμογών, όπου η πλειονότητα των εφαρμογών άμεσης ανταλλαγής μηνυμάτων και άλλων επιγραμμικών πλατφορμών χρησιμοποιούν επίσης τη διατερματική κρυπτογράφηση.

3. Προκλήσεις για τη διασφάλιση της ασφάλειας

Η «ψηφιακή ζωή» και ο κυβερνοχώρος δεν δημιουργούν μόνο τεράστιες ευκαιρίες, αλλά και σημαντικές προκλήσεις: η ψηφιοποίηση των σύγχρονων κοινωνιών οδηγεί σε τρωτά σημεία και ευκαιρίες εκμετάλλευσης για εγκληματικούς σκοπούς. Αυτό σημαίνει ότι οι εγκληματίες μπορούν να εντάξουν στους τρόπους δράσης τους άμεσα διαθέσιμες, έτοιμες προς χρήση λύσεις κρυπτογράφησης που έχουν σχεδιαστεί για νόμιμους σκοπούς[2].

Ταυτόχρονα, οι αρχές επιβολής του νόμου εξαρτώνται όλο και περισσότερο από την πρόσβαση σε ηλεκτρονικά πειστήρια για την αποτελεσματική καταπολέμηση της τρομοκρατίας, του οργανωμένου εγκλήματος, της σεξουαλικής κακοποίησης παιδιών (ιδίως των διαδικτυακών εκφάνσεών της), καθώς και μιας σειρά άλλων κυβερνοεγκλημάτων και εγκλημάτων που διευκολύνονται από τον κυβερνοχώρο. Για τις αρμόδιες αρχές, η πρόσβαση σε ηλεκτρονικά πειστήρια μπορεί να είναι ζωτικής σημασίας, όχι μόνον για τη διεξαγωγή επιτυχών ερευνών και, ως εκ τούτου, για την προσαγωγή των εγκληματιών στη δικαιοσύνη, αλλά επίσης για την προστασία των θυμάτων και τη διασφάλιση της ασφάλειας.

---

[1] Απόφαση της 16ης Ιουλίου 2020 στην υπόθεση C-311/18, Data Protection Commissioner κατά Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

[2] iOCTA 2020, σ. 25

Ωστόσο, υπάρχουν περιπτώσεις στις οποίες η κρυπτογράφηση καθιστά εξαιρετικά δύσκολη ή πρακτικά αδύνατη την πρόσβαση και την ανάλυση του περιεχομένου των επικοινωνιών στο πλαίσιο της πρόσβασης σε ηλεκτρονικά πειστήρια, παρόλο που πρόκειται για περιπτώσεις που η πρόσβαση στα εν λόγω δεδομένα θα ήταν νόμιμη. Ανεξάρτητα από το εκάστοτε τεχνολογικό πλαίσιο, είναι επομένως σημαντικό να διαφυλαχθούν οι εξουσίες των αρμόδιων αρχών στον τομέα της ασφάλειας και της ποινικής δικαιοσύνης μέσω νόμιμης πρόσβασης για την εκτέλεση των καθηκόντων τους, όπως προβλέπεται και επιτρέπεται από τον νόμο. Κάθε τέτοιος νόμος ο οποίος προβλέπει εξουσίες επιβολής πρέπει πάντα να σέβεται πλήρως την τήρηση της προσήκουσας διαδικασίας και άλλες εγγυήσεις, καθώς και τα θεμελιώδη δικαιώματα, ιδίως το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και των επικοινωνιών και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα.

4. Επίτευξη της ιδανικής ισορροπίας

Η αρχή της ασφάλειας μέσω κρυπτογράφησης και της ασφάλειας παρά την κρυπτογράφηση πρέπει να τηρείται στο σύνολό της. Η Ευρωπαϊκή Ένωση παραμένει υπέρ της ισχυρής κρυπτογράφησης. Η κρυπτογράφηση αποτελεί ακρογωνιαίο λίθο της εμπιστοσύνης στην ψηφιοποίηση και στην προστασία των θεμελιωδών δικαιωμάτων και θα πρέπει να προωθηθεί και να αναπτυχθεί.

Η προστασία της ιδιωτικής ζωής και της ασφάλειας των επικοινωνιών μέσω της κρυπτογράφησης και ταυτόχρονα η διατήρηση της δυνατότητας των αρμόδιων αρχών στον τομέα της ασφάλειας και της ποινικής δικαιοσύνης να έχουν νόμιμη πρόσβαση σε συναφή δεδομένα για νόμιμους και σαφώς καθορισμένους σκοπούς στο πλαίσιο της καταπολέμησης των σοβαρών και/ή οργανωμένων εγκλημάτων και της τρομοκρατίας, μεταξύ άλλων στον ψηφιακό κόσμο, και στην προάσπιση του κράτους δικαίου, είναι μείζονος σημασίας. Κάθε δράση που αναλαμβάνεται πρέπει να σταθμίζει προσεκτικά τα συμφέροντα αυτά με τις αρχές της αναγκαιότητας, της αναλογικότητας και της επικουρικότητας.

5. Συνένωση δυνάμεων με τον κλάδο της τεχνολογίας

Με το βλέμμα στραμμένο προς στο μέλλον, η Ευρωπαϊκή Ένωση προσπαθεί να εδραιώσει έναν δυναμικό διάλογο με τον τεχνολογικό κλάδο, διασυνδέοντας παράλληλα την έρευνα και την ακαδημαϊκή κοινότητα, ώστε να διασφαλιστεί η συνεχιζόμενη εφαρμογή και χρήση μιας ισχυρής τεχνολογίας κρυπτογράφησης. Οι αρμόδιες αρχές πρέπει να μπορούν να έχουν πρόσβαση στα δεδομένα με νόμιμο και στοχευμένο τρόπο, με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων και των σχετικών νόμων περί προστασίας των δεδομένων, διαφυλάσσοντας παράλληλα την ασφάλεια στον κυβερνοχώρο. Οι τεχνικές λύσεις για την απόκτηση πρόσβασης σε κρυπτογραφημένα δεδομένα πρέπει να συμμορφώνονται με τις αρχές της νομιμότητας, της διαφάνειας, της αναγκαιότητας και της αναλογικότητας, συμπεριλαμβανομένης της προστασίας των δεδομένων προσωπικού χαρακτήρα εκ σχεδιασμού και εξ ορισμού.

Δεδομένου ότι δεν υπάρχει ενιαίος τρόπος για την επίτευξη των τεθέντων στόχων, οι κυβερνήσεις, η βιομηχανία, η έρευνα και η ακαδημαϊκή κοινότητα πρέπει να συνεργαστούν με διαφάνεια για τη στρατηγική επίτευξη αυτής της ισορροπίας.

6. Κανονιστικό πλαίσιο

Θα μπορούσε να εξεταστεί περαιτέρω η ανάγκη εκπόνησης κανονιστικού πλαισίου για το σύνολο της ΕΕ, το οποίο θα επέτρεπε στις αρμόδιες αρχές να εκτελούν αποτελεσματικά τα επιχειρησιακά τους καθήκοντα, προστατεύοντας παράλληλα την ιδιωτική ζωή, τα θεμελιώδη δικαιώματα και την ασφάλεια της επικοινωνίας.

Οι δυνητικές τεχνικές λύσεις θα πρέπει να επιτρέπουν στις αρχές να ασκούν τις εξουσίες έρευνας που διαθέτουν, με σεβασμό στην αρχή της αναλογικότητας, της αναγκαιότητας και της δικαστικής εποπτείας βάσει της εθνικής τους νομοθεσίας, και με παράλληλο σεβασμό των κοινών ευρωπαϊκών αξιών και των θεμελιωδών δικαιωμάτων και διατήρηση των πλεονεκτημάτων της κρυπτογράφησης. Κάθε πιθανή λύση θα πρέπει να αναπτύσσεται με διαφανή τρόπο σε συνεργασία με τους εθνικούς και διεθνείς παρόχους υπηρεσιών επικοινωνίας και άλλους σχετικούς ενδιαφερόμενους φορείς. Οι εν λόγω τεχνικές λύσεις και πρότυπα — και η ταχεία ανάπτυξη της τεχνολογίας γενικότερα — προϋποθέτουν επίσης τη συνεχή βελτίωση των τεχνικών και επιχειρησιακών δεξιοτήτων και εμπειρογνωμοσύνης των αρμόδιων αρχών για την αποτελεσματική αντιμετώπιση των προκλήσεων της ψηφιοποίησης στο έργο τους σε παγκόσμια κλίμακα.

7. Καινοτόμες ερευνητικές ικανότητες

Τέλος, είναι μείζονος σημασίας να βελτιωθεί ο συντονισμός σε επίπεδο ΕΕ με στόχο:

1) τον συνδυασμό των προσπαθειών όλων των κρατών μελών και των θεσμικών οργάνων και οργανισμών της ΕΕ·

2) τον καθορισμό και την καθιέρωση καινοτόμων προσεγγίσεων καθώς αναδύονται νέες τεχνολογίες·

3) την ανάλυση κατάλληλων τεχνικών και επιχειρησιακών λύσεων· και

4) την παροχή εξατομικευμένης κατάρτισης υψηλής ποιότητας.

Θα πρέπει να εκπονηθούν τεχνικές και επιχειρησιακές λύσεις που θα βασίζονται σε ένα κανονιστικό πλαίσιο βασισμένο στις αρχές της νομιμότητας, της αναγκαιότητας και της αναλογικότητας, σε στενή διαβούλευση με τους παρόχους υπηρεσιών, άλλους σχετικούς ενδιαφερόμενους φορείς και όλες τις σχετικές αρμόδιες αρχές, αν και δεν θα πρέπει επιβληθεί μία ενιαία τεχνική λύση για την παροχή πρόσβασης σε κρυπτογραφημένα δεδομένα.

_____