

Η Σύμβαση του ΟΗΕ για το Κυβερνοέγκλημα

Μια ευκαιρία για την ανθρωπότητα να αντιμετωπίσει ένα σύγχρονο πρόβλημα.

Δεν έχουν περάσει πολλές μέρες από την εναρκτήρια διαδικασία της υπογραφής της Σύμβασης του ΟΗΕ για το Κυβερνοέγκλημα (**UN Convention against Cybercrime or Hanoi Convention**)¹, η οποία έλαβε χώρα στο **Ανόι** του Βιετνάμ, μετά από έναν μακροχρόνιο διάλογο στα όργανα του ΟΗΕ.

Σε μια εποχή κορύφωσης των νέων τεχνολογιών και συνεχούς αναδιαμόρφωσης του Κυβερνοχώρου δηλ. του ψηφιακού περιβάλλοντος που συγκροτούν οι δισεκατομμύρια συνδεδεμένες συσκευές και πλατφόρμες μαζί με το ανθρωπογενές πλαίσιο (*χρήστες της τεχνολογίας, καινοτόμοι δημιουργοί της τεχνολογίας*), αναδύονται νέες και σημαντικές προκλήσεις.

Το έγκλημα στον Κυβερνοχώρο, ως μια υψηλής απαξίας αντικοινωνική συμπεριφορά και ως μια ομολογία αποτυχίας της Κυβερνοασφάλειας, εξαπλώνεται ταχύτερα σήμερα, μέσα από την καθημερινή δράση εγκληματικών ομάδων που ακολουθούν επιχειρησιακά μοντέλα, υποστηριζόμενα από την τεχνολογία (ουσιαστικά μιλάμε για την κακή χρήση της τεχνολογίας).

Ταυτόχρονα οι επιπτώσεις από τον δυναμικό χαρακτήρα του Κυβερνοεγκλήματος είναι οδυνηρές για τις κοινωνίες και τα κράτη αφού διαπράττονται διαρκώς σοβαρά εγκλήματα, όπως η σεξουαλική εκμετάλλευση παιδιών, οι ποικιλόμορφες κυβερνοεπιθέσεις (σε βάρος ατόμων, εταιρειών και κρατών), οι διάφορες κατηγορίες απατών στον κυβερνοχώρο, η διακίνηση ναρκωτικών και ψυχότροπων ουσιών και ουσιών ντόπινγκ (μέσω του εμφανούς και μη διαδικτύου αλλά και η μεταφορά τους με νέα τεχνολογικά μέσα, σε μια εποχή «*delivery*»), η διακίνηση όπλων, η εμπορία ανθρώπων, παραβιάσεις της νομοθεσίας για την διανοητική ιδιοκτησία, ο διαδικτυακός τζόγος, η διακίνηση των fake news, η σύγχρονη τρομοκρατία (μέσα από την ριζοσπαστικοποίηση, την ανάπτυξη των ακραίων ιδεολογιών, την ρητορική του μίσους), κα.

Όλες οι επίσημες εκθέσεις των αρχών αντιμετώπισης του Κυβερνοεγκλήματος (**Cyber law Enforcement**)² και των διεθνών οργανισμών (ο ΟΗΕ³, το Συμβούλιο της Ευρώπης, η Ευρωπαϊκή Ένωση⁴, ο ΟΟΣΑ⁵, η Παγκόσμια Τράπεζα⁶, ASEAN⁷, κα) καταγράφουν με ακρίβεια την **αυξητική τάση** των εγκλημάτων στον Κυβερνοχώρο και ταυτόχρονα αναδεικνύουν την ανάγκη ύπαρξης ικανών κι αποτελεσματικών μηχανισμών αντιμετώπισης του Κυβερνοεγκλήματος.

Η διαπίστωση της ανάγκης αυτής έχει γίνει αντιληπτή από τους διεθνείς δρώντες χρονικά λίγο μετά την ανάπτυξη των νέων τεχνολογιών και για το λόγο αυτό έχουν υπάρξει και συνεχίζονται να υπάρχουν προσπάθειες, σε κρατικό και περιφερειακό επίπεδο, διαμόρφωσης κανονιστικού – θεσμικού πλαισίου.

Στην κατεύθυνση αυτή, ενδεικτικά αναφέρονται οι πρωτοβουλίες δημιουργίας κανόνων δικαίου, όπως η Σύμβαση για το Κυβερνοέγκλημα του Συμβουλίου της Ευρώπης (**Cybercrime Convention of Council of Europe- CoE or Budapest Convention**)⁸, η Σύμβαση για τα Φάρμακα που διακινούνται παράνομα στο διαδίκτυο (**Medicrime Convention of CoE**)⁹, οι πρωτοβουλίες για την αντιμετώπιση της ρητορικής του μίσους (hate speech)¹⁰, ο Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (General Data Protection Regulation - **GDPR**)¹¹ στο πλαίσιο λειτουργίας της ΕΕ, με συνολική αποτύπωση (**EUDPR**).

Επιπλέον, στην ίδια οπτική κατεύθυνση προτεραιοποιείται η δημιουργία ικανών μηχανισμών αντιμετώπισης του Κυβερνοεγκλήματος (**EC3- European Cybercrime Center**)¹² στο πλαίσιο της Europol, αλλά και της Eurojust (**EJCN – European Judicial Cybercrime Network**)¹³ σε δικαστικό επίπεδο, συμπληρωμένο από το αντίστοιχο μηχανισμό στο

πλαίσιο της **Interpol**¹⁴ για την εκτός της ΕΕ διεθνούς πραγματικότητας.

Η Σύμβαση του ΟΗΕ για το Κυβερνοέγκλημα (ή ακριβέστερα κατά του Κυβερνοεγκλήματος) έρχεται σήμερα όχι μόνο να συμπληρώσει αλλά να **ολοκληρώσει** αυτή την μερικώς προηγηθείσα συλλογική προσπάθεια των κρατικών και περιφερειακών οντοτήτων, με ένα χαρακτήρα καθολικό και οικουμενικό.

Ο βασικός λόγος που φτάσαμε στην σύμβαση αυτή είναι η ώριμη συνειδητοποίηση από όλα τα κράτη του πλανήτη που απαρτίζουν σήμερα τον Οργανισμό των Ηνωμένων Εθνών, ότι τελικά ο Κυβερνοχώρος καθίσταται ένας χώρος παγκόσμιος, ζωτικού χαρακτήρα για ολόκληρη την ανθρωπότητα.

Η καταπάτηση βασικών ανθρωπίνων δικαιωμάτων περνά σήμερα από την φυσική στην εικονική πραγματικότητα, όπου ατομικοί και συλλογικοί δράστες διαπράττουν πλέον σοβαρά εγκλήματα με την χρήση της εξελισσόμενης τεχνολογίας.

Οι ίδιοι εγκληματικοί δράστες τροφοδοτούν την γκρίζα οικονομία, αυξάνουν την κοινωνικοοικονομική ανισότητα σε βάρος ευάλωτων ανθρώπων (**παιδιά, ηλικιωμένα άτομα, γυναίκες, άτομα με αναπηρία, μετανάστες και πρόσφυγες**, κα), συντηρούν την διαφθορά και εμποδίζουν τις κοινωνίες να

ζήσουν ειρηνικά και να αναπτυχθούν επιτυγχάνοντας την ευημερία.

Για το λόγο αυτό η Σύμβαση φιλοδοξεί να βοηθήσει τα κράτη μέλη στην εναρμόνιση του θεσμικού πλαισίου (με απλούς και κοινά αποδεκτούς κανόνες), στην δημιουργία ικανών μηχανισμών διεθνούς συνεργασίας *[ανταλλαγής πληροφοριών, αμοιβαίας δικαστικής συνδρομής, τεχνικής βοήθειας και υποστήριξης σε σχέση με την εξιχνίαση των εγκλημάτων αυτών όπως χαρακτηριστική είναι η περίπτωση διαχείρισης των αποδεικτικών μέσων και πειστηρίων (e-evidence), την ανάπτυξη τεχνογνωσίας κι ανταλλαγής εξειδικευμένων γνώσεων]*.

Ωστόσο ο δρόμος μέχρι την ολοκλήρωση των σκοπών της Σύμβασης δεν είναι στρωμένος με ροδοπέταλα, αφού δεν πρέπει να ξεχνούμε κι άλλες παραμέτρους όπως οι συσχετισμοί δυνάμεων (σε οικονομικό, πολιτικό και τεχνολογικό επίπεδο), τα αντικρουόμενα ενδεχομένως συμφέροντα δυνάμεων (όπως οι ΗΠΑ, η Κίνα, η Ρωσία, η Ινδία, η ΕΕ, αλλά κι άλλων αναδυσόμενων στον 21^ο αιώνα δυνάμεων), που θα πρέπει να ξεπερνιούνται κάθε φορά για να προχωρήσει ουσιαστικά η συνεργασία.

Η χώρα μας συμμετείχε από την πρώτη στιγμή στις διεργασίες για την συγκεκριμένη σύμβαση και συγκαταλέγεται ανάμεσα στις χώρες που πρώτες υπέγραψαν την συγκεκριμένη Σύμβαση¹⁵, αυξάνοντας θετικά την διεθνή εικόνα της χώρας μας.



Representative of Greece signs the United Nations Convention against Cybercrime.

Πηγή φωτογραφίας¹⁶:

Ωστόσο για να ολοκληρώσει η χώρα μας την προσπάθεια αυτή θα πρέπει να κινηθεί με γρηγορότερους ρυθμούς σε μια σειρά από μέτρα που θα προετοιμάσουν καλύτερα και θα αυξήσουν την ικανότητα ανταπόκρισης και διαχείρισης των περιστατικών Κυβερνοεγκλημάτων που τελούνται σε βάρος ανθρώπων που ζουν στη χώρα μας.

Συγκεκριμένα θα πρέπει να:

- επικυρώσει από τη Βουλή τη Σύμβαση για τα φάρμακα που διακινούνται παράνομα στο διαδίκτυο
- αναμορφώσει το ποινικό και δικονομικό πλαίσιο (καθιέρωση ειδικού εισαγγελέα για τα εγκλήματα στον Κυβερνοχώρο, εξειδίκευση δικαστών, καθιέρωση της

άυλης δικογραφίας, επιτάχυνση της ψηφιοποίησης των δικαστηρίων, ενσωμάτωση εργαλείων όπως η Τεχνητή Νοημοσύνη στην δικαστηριακή πρακτική, κα)

- δημιουργήσει και ενισχύσει ένα πλαίσιο πρόληψης μέσα από την εκπαίδευση και την ανάπτυξη ψηφιακών ικανοτήτων για όλα τα άτομα και ιδιαίτερα αυτά που χαρακτηρίζονται ως ευάλωτα (με την αξιοποίηση εκπαιδευτικών κι ερευνητικών πόρων, ενεργοποίηση θεσμών όπως η τοπική αυτοδιοίκηση, τα επιμελητήρια, οι βιβλιοθήκες, η εκκλησία, κα).
- Δημιουργία εθνικής στρατηγικής για μια κουλτούρα τεχνοηθικής (μέρος της βιοηθικής) υπηρετώντας το τρίπτυχο της **αξιοκρατίας-διαφάνειας-δικαιοσύνης**

Η σύμβαση του ΟΗΕ για το κυβερνοέγκλημα είναι μια ευκαιρία ακόμη τόσο για την χώρα μας όσο και για όλη την ανθρωπότητα να περιορίσουν τον αρνητικό αντίκτυπο της κακής χρήση της τεχνολογίας και να αυξήσουν την θετική και δημιουργική χρήση της με επίκεντρο τον άνθρωπο.

Κι αυτό δεν ενώνει μόνο τα έθνη – κράτη μέλη του Οργανισμού των Ηνωμένων Εθνών αλλά όλους τους ανθρώπους που θέλουν **να χωρούν στον Κυβερνοχώρο** με αξιοπρέπεια κι ελευθερία.

Γιώργος Παπαπροδρόμου

Αντιστράτηγος ε.α.{ΕΛ.ΑΣ.]

Πτυχιούχος Νομικής ΑΠΘ – Δικαστικός Γραφολόγος

Ειδικός σε θέματα Αντιμετώπισης Κυβερνοεγκλήματος

Πηγές

¹ <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>

² <https://www.europol.europa.eu/publications-events/main-reports/iocta-report> & https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf & https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

³ <https://www.unodc.org/romena/en/cybercrime.html>

⁴ https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

⁵ <https://www.oecd.org/en/topics/digital-security.html>

⁶ <https://id4d.worldbank.org/guide/cybercrime-and-cybersecurity>

⁷ <https://cybilportal.org/projects/asean-cybercrime-operations-desk/>

⁸ <https://www.coe.int/en/web/cybercrime>

⁹ <https://www.coe.int/en/web/medicrime/the-medicrime-convention>

¹⁰ <https://www.coe.int/en/web/combating-hate-speech>

¹¹ https://commission.europa.eu/law/law-topic/data-protection_en

¹² <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

¹³ <https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/european-judicial-cybercrime-network>

¹⁴ <https://www.interpol.int/Crimes/Cybercrime>

¹⁵ <https://news.un.org/en/story/2025/10/1166182> &

https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-16&chapter=18&clang=en & <https://vietnamnews.vn/politics-laws/1728082/countries-signed-the-un-convention-against-convention-in-ha-noi-ceremony.html>

¹⁶ <https://vietnamnews.vn/politics-laws/1728082/countries-signed-the-un-convention-against-convention-in-ha-noi-ceremony.html>