ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ

Βρυξέλλες, 26.1.2001
COM(2000) 890 τελικό

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΣΥΜΒΟΥΛΙΟ, ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΣΤΗΝ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΣΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Για μια ασφαλέστερη Κοινωνία της Πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής

eEurope 2002

Σύνοψη

Η μετατροπή της Ευρώπης σε κοινωνία της πληροφορίας χαρακτηρίζεται από βαθιές εξελίξεις σε όλους τους τομείς της ανθρώπινης ζωής: εργασία, εκπαίδευση και ψυχαγωγία, κυβερνητικό σύστημα, βιομηχανία και εμπόριο. Οι νέες τεχνολογίες πληροφόρησης και επικοινωνίας έχουν επαναστατική και θεμελιώδη επίπτωση στις οικονομίες μας και τις κοινωνίες μας. Η επιτυχία της κοινωνίας της πληροφορίας είναι σημαντική για την ανάπτυξη, την ανταγωνιστικότητα και τις ευκαιρίες απασχόλησης της Ευρώπης και έχει σημαντικές οικονομικές, κοινωνικές και νομικές επιπτώσεις.

Η Επιτροπή ξεκίνησε την πρωτοβουλία *e*-Europe τον Δεκέμβριο του 1999 για να εξασφαλίσει ότι η Ευρώπη μπορεί να αποκομίσει τα οφέλη των ψηφιακών τεχνολογιών και ότι η κοινωνία της πληροφορίας δεν δημιουργεί κοινωνικό αποκλεισμό. Τον Ιούνιο του 2000, το Ευρωπαϊκό Συμβούλιο της Φέιρα ενέκρινε ένα συνοπτικό πρόγραμμα δράσης *e*-Europe και ζήτησε την εφαρμογή του πριν από τα τέλη του 2002. Το πρόγραμμα δράσης τονίζει τη σημασία της ασφάλειας του δικτύου και της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

Οι υποδομές πληροφόρησης και επικοινωνίας έχουν καταστεί ουσιαστικό τμήμα των οικονομιών μας. Δυστυχώς, αυτές οι υποδομές έχουν τα δικά τους αδύνατα σημεία και προσφέρουν νέες ευκαιρίες για εγκληματικές συμπεριφορές. Αυτές οι εγκληματικές δραστηριότητες μπορούν να λάβουν διάφορες μορφές και να διασχίσουν πολλά σύνορα. Παρά το γεγονός ότι, για σειρά λόγων, δεν υπάρχουν αξιόπιστες στατιστικές, είναι αναμφίβολο ότι αυτά τα αδικήματα αποτελούν απειλή για τις βιομηχανικές επενδύσεις και κεφάλαια και για την ασφάλεια και εμπιστοσύνη στην κοινωνία της πληροφορίας. Ορισμένα πρόσφατα παραδείγματα επιθέσεων ιών και άρνησης παροχής υπηρεσίας έχει αναφερθεί ότι έχουν προξενήσει σημαντικές οικονομικές ζημιές.

Υπάρχει πεδίο δράσης τόσο από την άποψη της πρόληψης των εγκληματικών δραστηριοτήτων με την ενίσχυση της ασφάλειας των υποδομών πληροφόρησης όσο και από την άποψη της εξασφάλισης στις αρχές εφαρμογής του νόμου των απαραίτητων μέσων δράσης, ενώ ταυτόχρονα θα τηρούνται πλήρως τα θεμελιώδη δικαιώματα των ατόμων.

Η Ευρωπαϊκή Ένωση έχει ήδη θεσπίσει σειρά μέτρων για την καταπολέμηση του παράνομου και επιζήμιου περιεχομένου του Διαδικτύου, για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας και των δεδομένων προσωπικού χαρακτήρα, για την προώθηση του ηλεκτρονικού εμπορίου και τη χρήση των ηλεκτρονικών υπογραφών, και για την ενίσχυση της ασφάλειας των συναλλαγών. Τον Απρίλιο του 1998, η Επιτροπή παρουσίασε στο Συμβούλιο τα αποτελέσματα μελέτης για το έγκλημα πληροφορικής (μελέτη 'COMCRIME'). Τον Οκτώβριο 1999, το Ευρωπαϊκό Συμβούλιο του Τάμπερε όρισε ότι οι προσπάθειες να επιτευχθεί συμφωνία για κοινούς ορισμούς και κυρώσεις πρέπει να αφορούν εξίσου τα εγκλήματα υψηλής τεχνολογίας. Το Ευρωπαϊκό Κοινοβούλιο απηύθυνε επίσης έκκληση για κοινά παραδεκτούς ορισμούς των εγκλημάτων πληροφορικής και για πραγματική προσέγγιση των νομοθεσιών, ιδιαίτερα όσον αφορά το ποινικό δίκαιο. Το Συμβούλιο της Ευρωπαϊκής Ένωσης εξέδωσε κοινή θέση σχετικά με τις διαπραγματεύσεις που αφορούν το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και έλαβε ορισμένα αρχικά μέτρα στο πλαίσιο της στρατηγικής της Ένωσης για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας. Ορισμένα κράτη μέλη της Ευρωπαϊκής Ένωσης διαδραμάτισαν επίσης πρωτεύοντα ρόλο στις σχετικές με το θέμα δραστηριότητες των χωρών του G8 .

Η παρούσα ανακοίνωση εξετάζει την ανάγκη να υπάρξει πρωτοβουλία προκειμένου να καθορισθεί συνολική πολιτική καθώς και τις διάφορες μορφές που μπορεί αυτή να λάβει, στο πλαίσιο ευρύτερων στόχων που συνιστούν *την κοινωνία της πληροφορίας* και *τη δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης*, προκειμένου να βελτιωθεί η ασφάλεια των υποδομών πληροφόρησης και να καταπολεμηθεί το έγκλημα πληροφορικής, σύμφωνα προς τη δέσμευση της Ευρωπαϊκής Ένωσης για την τήρηση των θεμελιωδών ανθρωπίνων δικαιωμάτων.

Η Επιτροπή θεωρεί ότι βραχυπρόθεσμα υπάρχει σαφής ανάγκη για κοινοτικό μέσο που θα εξασφαλίζει ότι τα κράτη μέλη διαθέτουν αποτελεσματικές κυρώσεις για την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο. Θα παρουσιάσει πριν από τα τέλη του έτους πρόταση απόφασης-πλαισίου που θα περιλαμβάνει, στο ευρύτερο πλαίσιο ενός πακέτου που θα καλύπτει θέματα σχετικά με την σεξουαλική εκμετάλλευση των παιδιών και την εμπορία ανθρώπων, διατάξεις με σκοπό την προσέγγιση των νομοθεσιών και των κυρώσεων.

Πιο μακροπρόθεσμα, η Επιτροπή θα υποβάλει νομοθετικές προτάσεις για την περαιτέρω προσέγγιση του ποινικού δικαίου στον τομέα του εγκλήματος υψηλής τεχνολογίας. Σύμφωνα με τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου του Τάμπερε του Οκτωβρίου 1999, η Επιτροπή θα εξετάσει επίσης πιθανά μέτρα για την αμοιβαία αναγνώριση των αποφάσεων που προηγούνται της δικαστικής φάσης οι οποίες έχουν σχέση με ανακρίσεις για εγκλήματα πληροφορικής.

Παράλληλα, η Επιτροπή προτίθεται να προωθήσει σε εθνικό επίπεδο τη δημιουργία αστυνομικών μονάδων εξειδικευμένων στην καταπολέμηση των εγκλημάτων πληροφορικής, εκεί όπου δεν υπάρχουν ακόμα τέτοιες μονάδες, να υποστηρίξει τις κατάλληλες ενέργειες τεχνικής κατάρτισης για την εφαρμογή του νόμου και να ενθαρρύνει τις ευρωπαϊκές πρωτοβουλίες στον τομέα της ασφάλειας της πληροφόρησης.

Σε τεχνικό επίπεδο, και σύμφωνα με το νομικό πλαίσιο, η Επιτροπή θα ενθαρρύνει τις προσπάθειες έρευνας και ανάπτυξης για την κατανόηση και μείωση των αδυναμιών και θα προωθήσει τη διάδοση τεχνογνωσίας.

Η Επιτροπή προτίθεται επίσης να δημιουργήσει ένα φόρουμ της Ευρωπαϊκής Ένωσης το οποίο θα συγκεντρώνει τις αρχές εφαρμογής του νόμου, τους παρόχους υπηρεσιών Διαδικτύου, τις επιχειρήσεις τηλεπικοινωνιών, τις οργανώσεις πολιτικών ελευθεριών, τους αντιπροσώπους των καταναλωτών, τις αρχές που είναι επιφορτισμένες με την προστασία των δεδομένων, και άλλους ενδιαφερόμενους με στόχο να βελτιώσει την αμοιβαία κατανόηση και τη συνεργασία στο επίπεδο της Ευρωπαϊκής Ένωσης. Αυτό το φόρουμ θα προσπαθήσει να ευαισθητοποιήσει το κοινό για τους κινδύνους εγκληματικότητας στο Διαδίκτυο, να προωθήσει τις βέλτιστες πρακτικές στον τομέα της ασφάλειας, να προσδιορίσει αποτελεσματικά μέσα και διαδικασίες για την καταπολέμηση των εγκλημάτων πληροφορικής και να ενθαρρύνει την περαιτέρω ανάπτυξη μηχανισμών έγκαιρης προειδοποίησης και διαχείρισης κρίσεων.

ΠΡΟΣΚΛΗΣΗ ΓΙΑ ΤΗΝ ΥΠΟΒΟΛΗ ΠΑΡΑΤΗΡΗΣΕΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΝΑΚΟΙΝΩΣΗ

Η Ευρωπαϊκή Επιτροπή καλεί όλους τους ενδιαφερομένους να υποβάλουν παρατηρήσεις για όλα τα θέματα που αναλύονται στην παρούσα ανακοίνωση. Οι παρατηρήσεις μπορούν να αποσταλούν μέχρι τις 23.03.2001 με ηλεκτρονικό ταχυδρομείο στην ακόλουθη διεύθυνση:

Infso-jai-cybercrime-comments@cec.eu.int

Οι παρατηρήσεις θα δημοσιευθούν κατ΄ αρχήν στο Διαδίκτυο, εκτός εάν ο αποστολέας ζητήσει ρητά τη μη δημοσίευση τους. Ανώνυμες παρατηρήσεις δεν θα δημοσιευθούν. Η Επιτροπή επιφυλάσσει το δικαίωμα να μη δημοσιεύσει παρατηρήσεις που θα λάβει (π.χ. παρατηρήσεις προσβλητικού περιεχομένου). Οι παρατηρήσεις θα διατίθενται στην ακόλουθη ιστοθέση:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

Υποδείξεις όσον αφορά το τεχνικό μορφότυπο και λεπτομέρειες της πολιτικής δημοσιεύσεων θα διατίθενται στη συγκεκριμένη ιστοθέση. Παρακαλείσθε να ελέγξετε την ιστοθέση πριν να αποστείλετε τις παρατηρήσεις σας.

ΔΗΜΟΣΙΑ ΑΚΡΟΑΣΗ

Η Ευρωπαϊκή Επιτροπή θα διοργανώσει επίσης δημόσια ακρόαση των ενδιαφερομένων για τα θέματα που αναλύονται στην ανακοίνωση. Αυτή η ακρόαση θα πραγματοποιηθεί την 07.03.2001. Οι αιτήσεις για πρόσκληση με σκοπό την υποβολή παρατηρήσεων κατά τη συγκεκριμένη ακρόαση πρέπει να αποσταλούν μέχρι τις 20.02.2001 με ηλεκτρονικό ταχυδρομείο στην ακόλουθη διεύθυνση:

Infso-jai-cybercrime-hearing@cec.eu.int

ή ταχυδρομικά στη διεύθυνση:

European Commission
Office BU33-5/9
200 Wetstraat/Rue de la Loi
B-1049 Brussels
Belgium

Η Ευρωπαϊκή Επιτροπή επιφυλάσσει το δικαίωμα να προβεί σε επιλογή των μερών που θα συμμετάσχουν στην ακρόαση. Οποιαδήποτε επιλογή θα στηριχθεί στον αριθμό των αιτήσεων και στην επιθυμία να υπάρξει ευρεία κάλυψη συμφερόντων.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΥΚΑΙΡΙΕΣ ΚΑΙ ΑΠΕΙΛΕΣ ΣΤΗΝ ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

Η αυξανόμενη διαθεσιμότητα και χρήση των τεχνολογιών της Κοινωνίας της Πληροφορίας (ΤΚΠ) και η παγκοσμιοποίηση της οικονομίας αποτελούν χαρακτηριστικά της περιόδου την οποία διανύουμε. Η περαιτέρω τεχνολογική ανάπτυξη και η αυξημένη χρήση των ανοικτών δικτύων, όπως το Διαδίκτυο, κατά τα επόμενα έτη θα δημιουργήσουν νέες σημαντικές δυνατότητες και θα θέσουν νέες προκλήσεις.

Το Ευρωπαϊκό Συμβούλιο της Λισσαβόνας, το Μάρτιο 2000, τόνισε τη σημασία την οποία έχει η μετάβαση προς μια ανταγωνιστική, δυναμική και θεμελιωμένη στη γνώση οικονομία και κάλεσε το Συμβούλιο και την Επιτροπή να εκπονήσουν πρόγραμμα δράσης για μια ηλεκτρονική Ευρώπη (*e*Europe Action plan) για να αξιοποιηθεί στο μέγιστο αυτή η ευκαιρία.[1] Αυτό το πρόγραμμα δράσης, το οποίο καταρτίστηκε από την Επιτροπή και το Συμβούλιο και εγκρίθηκε από το Ευρωπαϊκό Συμβούλιο της Φέιρα τον Ιούνιο 2000, περιλαμβάνει ενέργειες που αποβλέπουν στην ενίσχυση της ασφάλειας των δικτύων και προβλέπει την ανάπτυξη συντονισμένης και συνεκτικής προσέγγισης του εγκλήματος στον κυβερνοχώρο μέχρι τα τέλη του 2002.[2]

Οι υποδομές πληροφόρησης αποτελούν τη ραχοκοκαλιά των οικονομιών μας. Οι χρήστες πρέπει να μπορούν να υπολογίζουν στην διαθεσιμότητα υπηρεσιών πληροφόρησης και να έχουν εμπιστοσύνη στο γεγονός ότι οι επικοινωνίες τους και τα δεδομένα τους θα προστατεύονται κατά οποιασδήποτε μη εξουσιοδοτημένης πρόσβασης ή τροποποίησης. Η ανάπτυξη του ηλεκτρονικού εμπορίου και η πλήρης υλοποίηση της Κοινωνίας της Πληροφορίας εξαρτάται από αυτό.

Οι νέες ψηφιακές και ασύρματες τεχνολογίες υπάρχουν ήδη παντού. Μας παρέχουν τη δυνατότητα κινητικότητας, παραμένοντας πάντα συνδεδεμένοι με μυριάδες υπηρεσιών προσβάσιμων από δίκτυα δικτύων. Μας παρέχουν επίσης τη δυνατότητα συμμετοχής, διδασκαλίας και εκμάθησης, από κοινού εργασίας και παιγνιδιού, συμμετοχής στην πολιτική διαδικασία. Στο μέτρο εντούτοις που οι κοινωνίες θα εξαρτηθούν περισσότερο από αυτήν την τεχνική, θα πρέπει να χρησιμοποιηθούν πρακτικά και νομικά μέσα για να αντιμετωπιστούν οι κίνδυνοι που συνδέονται με αυτή την εξέλιξη.

Οι Τεχνολογίες της Κοινωνίας της Πληροφορίας (ΤΚΠ) μπορούν να χρησιμοποιηθούν και χρησιμοποιούνται πράγματι για τη διάπραξη και τη διευκόλυνση διαφόρων εγκληματικών δραστηριοτήτων. Στα χέρια ατόμων που δρουν κακόπιστα, κακόβουλα ή με σοβαρή αμέλεια, αυτές οι τεχνολογίες μπορούν να καταστούν εργαλεία για δραστηριότητες που θέτουν σε κίνδυνο τη ζωή, τα αγαθά ή την αξιοπρέπεια ατόμων ή να θίξουν το δημόσιο συμφέρον.

Η κλασσική προσέγγιση όσον αφορά την ασφάλεια απαιτούσε την αυστηρή οργανωτική, γεωγραφική και διαρθρωτική στεγανοποίηση των πληροφοριών ανάλογα με την ευαισθησία και την κατηγορία τους. Αυτή η προσέγγιση είναι ξεπερασμένη στον ψηφιακό κόσμο δεδομένου ότι η επεξεργασία της πληροφορίας είναι κατανεμημένη, οι υπηρεσίες παρέχονται σε χρήστες κινητών επικοινωνιών και η διαλειτουργικότητα των συστημάτων αποτελεί προαπαιτούμενο. Καινοτόμες λύσεις βασισμένες στις νεοεμφανιζόμενες τεχνολογίες

---

1 Συμπεράσματα της Προεδρίας του Ευρωπαϊκού Συμβουλίου της Λισσαβόνας της 23ης και 24ης Μαρτίου 2000, διαθέσιμα στην ιστοσελίδα http://ue.eu.int/en/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm.

υποκαθίστανται στις κλασσικές προσεγγίσεις που αφορούν τα ζητήματα ασφάλειας. Περιλαμβάνουν τη χρήση τεχνικών κρυπτογράφησης και ψηφιακών υπογραφών, νέα εργαλεία ελέγχου της πρόσβασης και της γνησιότητας, καθώς επίσης όλα τα είδη φίλτρων λογισμικού[3]. Οι ασφαλείς και αξιόπιστες υποδομές πληροφόρησης απαιτούν όχι μόνο την ύπαρξη κλίμακας τεχνολογιών αλλά εξίσου τη σωστή και αποτελεσματική χρήση τους. Ορισμένες από αυτές τις τεχνολογίες υπάρχουν ήδη, αλλά οι χρήστες αγνοούν συχνά την ύπαρξή τους, τον τρόπο χρήσης τους, ή τους λόγους για τους οποίους αυτές μπορούν να είναι απαραίτητες.

1.1. Απαντήσεις σε εθνικό και διεθνές επίπεδο

Το έγκλημα πληροφορικής επηρεάζει όλο τον κυβερνοχώρο και δεν σταματά στα παραδοσιακά σύνορα των κρατών. Αυτές οι παραβάσεις μπορούν κατ΄ αρχήν να διαπράττονται από οποιοδήποτε σημείο εις βάρος οποιουδήποτε χρήστη υπολογιστή, οπουδήποτε και εάν αυτός ευρίσκεται. Έχει γενικά αναγνωριστεί ότι χρειάζεται αποτελεσματική δράση για την καταπολέμηση του εγκλήματος πληροφορικής τόσο σε εθνικό όσο και σε διεθνές επίπεδο[4].

Σε εθνικό επίπεδο λείπουν συχνά ολοκληρωμένες απαντήσεις που να λαμβάνουν υπόψη τη διεθνή διάσταση για να αντιμετωπίσουν τις νέες προκλήσεις που είναι η ασφάλεια των δικτύων και το έγκλημα πληροφορικής. Στα περισσότερα κράτη, οι αντιδράσεις στο έγκλημα πληροφορικής βασίζονται στο εθνικό δίκαιο (ειδικότερα το ποινικό δίκαιο) και παραμελούν άλλα εναλλακτικά προληπτικά μέτρα.

Παρά τις προσπάθειες διεθνών και υπερεθνικών οργανώσεων, οι διάφορες εθνικές νομοθεσίες παγκοσμίως παρουσιάζουν σημαντικές διαφορές, ιδιαίτερα όσον αφορά τις διατάξεις ποινικού δικαίου, την ηλεκτρονική πειρατεία, την προστασία των επαγγελματικών απορρήτων και το παράνομο περιεχόμενο. Υπάρχουν επίσης σημαντικές διαφορές όσον αφορά τις εξουσίες εξαναγκασμού των ανακριτικών υπηρεσιών (ειδικότερα όσον αφορά τα κρυπτογραφημένα δεδομένα και τις έρευνες στα διεθνή δίκτυα), την έκταση της ποινικής αρμοδιότητας, καθώς και την ευθύνη των ενδιάμεσων φορέων παροχής υπηρεσιών αφενός, και των φορέων παροχής περιεχομένου αφετέρου. Η οδηγία 2000/31/ΕΚ[5] για το ηλεκτρονικό εμπόριο τροποποιεί αυτή την κατάσταση όσον αφορά την ευθύνη των ενδιάμεσων φορέων παροχής υπηρεσιών για ορισμένες διαμεσολαβητικές δραστηριότητες. Αυτή η οδηγία απαγορεύει εξάλλου στα κράτη μέλη να επιβάλουν σε αυτούς τους παρόχους υπηρεσιών τη γενική υποχρέωση να ελέγχουν τις πληροφορίες που διαβιβάζουν ή αποθηκεύουν.

---

[3] Οι ροές πληροφόρησης φιλτράρονται και ελέγχονται σε όλα τα επίπεδα· από τη ζώνη ασφάλειας που εξετάζει τα πακέτα δεδομένων, το φίλτρο που εξετάζει τα κακόβουλα προγράμματα, το φίλτρο ηλεκτρονικού ταχυδρομείου που εξαλείφει το μη ζητηθέν ηλεκτρονικό ταχυδρομείο, μέχρι το φίλτρο διαφυλιστή (browser) που αποτρέπει την πρόσβαση σε επιζήμιο υλικό.

[4] Βλέπε, π.χ., το σχέδιο δράσης *e*-Europe στη διεύθυνση: http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm, και δηλώσεις του Επιτρόπου Antõnio Vitorino στη διεύθυνση: http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf, και του γάλλου Πρωθυπουργού Lionel Jospin στη διεύθυνση. http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

[5] Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 σχετικά με ορισμένα νομικά ζητήματα των υπηρεσιών της κοινωνίας της πληροφορίας, και κυρίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά ("Οδηγία για το ηλεκτρονικό εμπόριο").

Σε διεθνές και υπερεθνικό επίπεδο, η ανάγκη να καταπολεμηθεί αποτελεσματικά το έγκλημα πληροφορικής έχει ευρέως αναγνωριστεί και διάφοροι οργανισμοί συντονίζουν ή προσπαθούν να εναρμονίσουν τις δραστηριότητές τους στο συγκεκριμένο τομέα. Οι υπουργοί δικαιοσύνης και εσωτερικών υποθέσεων των χωρών του G8 θέσπισαν σύνολο αρχών και ένα σχέδιο δράσης σε 10 σημεία το Δεκέμβριο του 1997, το οποίο επικυρώθηκε από τη διάσκεψη κορυφής του G8 στο Birmingham τον Ιούνιο του 1998 και ευρίσκεται τώρα στο στάδιο της εφαρμογής.[6] Το Συμβούλιο της Ευρώπης ξεκίνησε να προετοιμάζει μια διεθνή σύμβαση για το έγκλημα στο κυβερνοχώρο το Φεβρουάριο του 1997 και αναμένεται να ολοκληρώσει αυτό το καθήκον μέχρι τα τέλη του έτους 2001.[7] Η καταπολέμηση του εγκλήματος πληροφορικής συμπεριλαμβάνεται επίσης στην ημερήσια διάταξη διμερών συζητήσεων της Ευρωπαϊκής Επιτροπής με ορισμένες κυβερνήσεις, εκτός Ευρωπαϊκής Ένωσης. Έχει δημιουργηθεί μια κοινή Task Force ΕΚ/ΗΠΑ για την προστασία των κρίσιμων υποδομών (Critical Infrastructure Protection)[8]. Τα Ηνωμένα Έθνη και ο ΟΟΣΑ έχουν επίσης αναλάβει δράση στο συγκεκριμένο τομέα και γίνονται συζητήσεις σε διεθνή φόρα όπως το Global Business Dialogue και το Tras-Antlantic Business Dialogue.[9]

Στην Ευρωπαϊκή Ένωση, μέχρι πρόσφατα, τα θεσπιζόμενα νομοθετικά μέτρα αφορούσαν κυρίως τους τομείς των δικαιωμάτων πνευματικής ιδιοκτησίας, της θεμελιώδους αρχής της προστασίας του ιδιωτικού βίου και της προστασίας των δεδομένων, των υπηρεσιών με υπό όρους πρόσβαση, του ηλεκτρονικού εμπορίου, των ηλεκτρονικών υπογραφών και ιδιαίτερα την απελευθέρωση του εμπορίου των συστημάτων κρυπτογράφησης, που συνδέονται έμμεσα με το έγκλημα πληροφορικής .

Κατά τα τελευταία 3-4 έτη έχουν επίσης ληφθεί ορισμένα σημαντικά νομοθετικά μέτρα. Αυτά συμπεριλαμβάνουν το πρόγραμμα δράσης για την καταπολέμηση του παράνομου και επιζήμιου περιεχομένου του Διαδικτύου, το οποίο συγχρηματοδοτεί ενέργειες ευαισθητοποίησης, δοκιμές ταξινόμησης και φιλτραρίσματος του περιεχομένου και των απευθείας συνδέσεων (hot-lines) και πρωτοβουλίες σχετικά με την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στην κοινωνία της πληροφορίας, την παιδική πορνογραφία και την παρακολούθηση επικοινωνιών για λόγους εφαρμογής του νόμου[10]. Η Ευρωπαϊκή

---

6 Το Συμβούλιο ΔΕΥ της Ευρωπαϊκής Ένωσης της 19ης Μαρτίου 1998 υιοθέτησε τις 10 αρχές του G8 σχετικά με το έγκλημα υψηλής τεχνολογίας και κάλεσε τα κράτη μέλη της Ευρωπαϊκής Ένωσης που δε συμμετέχουν στο G8 να πράξουν τα δέοντα για να προσχωρήσουν στο δίκτυο.
Διατίθεται στην ιστοθέση Ευρωπαϊκό Δικαστικό Δίκτυο http://ue.eu.int/ejn/index.htm.

7 Το σχέδιο σύμβασης διατίθεται στο δίκτυο σε δυο γλώσσες: στα γαλλικά, στη διεύθυνση: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm.
και στα αγγλικά, στη διεύθυνση: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

8 Υπό την αιγίδα της Κοινής Συμβουλευτικής Ομάδας της Συμφωνίας ΕΚ/ΗΠΑ Επιστημονική και Τεχνολογική Συνεργασία.

9 Τα Ηνωμένα Έθνη έχουν συντάξει λεπτομερές εγχειρίδιο με τον τίτλο "Εγχειρίδιο για την πρόληψη και τον έλεγχο του εγκλήματος πληροφορικής", το οποίο ενημερώθηκε πρόσφατα. Το 1983, ο ΟΟΣΑ πραγματοποίησε μελέτη για τις δυνατότητες διεθνούς εφαρμογής και εναρμόνισης των ποινικών νομοθεσιών προκειμένου να αντιμετωπισθεί το πρόβλημα του εγκλήματος ή των καταχρήσεων πληροφορικής. Το 1986, δημοσίευσε έκθεση με τον τίτλο "Computer-Related Crime: Analysis of Legal Policy", όπου εξέταζε τις ισχύουσες νομοθεσίες και τις προτάσεις αναθεώρησης σε ορισμένα κράτη μέλη και συνέστηνε έναν ελάχιστο κατάλογο καταχρήσεων τις οποίες τα κράτη θα έπρεπε να θεωρούν απαγορευμένες και αξιόποινες σύμφωνα με το ποινικό τους δίκαιο. Τέλος το 1992, ο ΟΟΣΑ όρισε ένα σύνολο κατευθυντήριων γραμμών που διέπουν την ασφάλεια των ηλεκτρονικών συστημάτων, οι οποίες προορίζονται να χρησιμεύσουν ως βάση για την δημιουργία, από τα κράτη και τον ιδιωτικό τομέα, ενός πλαισίου για την ασφάλεια των συστημάτων πληροφόρησης.

10 Σύσταση 98/560/ΕΚ του Συμβουλίου της 24ης Σεπτεμβρίου 1998 για την ανάπτυξη της ανταγωνιστικότητας της ευρωπαϊκής βιομηχανίας των οπτικοακουστικών υπηρεσιών και της πληροφορίας με την προώθηση εθνικών πλαισίων που αποβλέπουν στην κατοχύρωση συγκρίσιμου και αποτελεσματικού επιπέδου προστασίας των ανηλίκων και της ανθρώπινης αξιοπρέπειας· Πράσινο

Ένωση υποστηρίζει από καιρό σχέδια έρευνας και ανάπτυξης που αποβλέπουν στην προώθηση της ασφάλειας και της εμπιστοσύνης στις υποδομές πληροφόρησης και τις ηλεκτρονικές συναλλαγές και αύξησε πρόσφατα τα κονδύλια προϋπολογισμού για το πρόγραμμα ΤΚΠ. Τα σχέδια έρευνας και τα λειτουργικά σχέδια που προορίζονται να προωθήσουν την εξειδικευμένη κατάρτιση του προσωπικού των υπηρεσιών καταστολής του εγκλήματος καθώς και τη συνεργασία μεταξύ αυτών των υπηρεσιών και των επιχειρήσεων αποτελούν εξίσου το αντικείμενο ενίσχυσης στο πλαίσιο προγραμμάτων που υπάγονται στον τρίτο πυλώνα όπως το STOP, FALCONE, OISIN και GROTIUS.[11]

Το σχέδιο δράσης για την καταπολέμηση του οργανωμένου εγκλήματος, που θεσπίστηκε από το Συμβούλιο ΔΕΥ το Μάιο 1997 και εγκρίθηκε από το Ευρωπαϊκό Συμβούλιο του Άμστερνταμ, καλούσε την Επιτροπή επεξεργασθεί μελέτη για το έγκλημα πληροφορικής μέχρι τα τέλη του 1998. Αυτή η μελέτη, γνωστή ως 'μελέτη COMCRIME,' υποβλήθηκε από την Επιτροπή στην πολυθεματική ομάδα εργασίας του Συμβουλίου κατά του οργανωμένου εγκλήματος τον Απρίλιο του 1998. [12] Η παρούσα ανακοίνωση αποτελεί εν μέρει συνέχεια του αιτήματος του Συμβουλίου ΔΕΥ.

Η Επιτροπή, πριν από τη σύνταξη της παρούσας ανακοίνωσης, έκρινε απαραίτητο να πραγματοποιήσει άτυπες διαβουλεύσεις με αντιπροσώπους των αρχών εφαρμογής του νόμου και των αρχών ελέγχου για την προστασία ων δεδομένων[13] καθώς και με αντιπροσώπους των ευρωπαϊκών επιχειρήσεων (ως επί το πλείστον φορείς παροχής υπηρεσιών στο Διαδίκτυο και επιχειρήσεις τηλεπικοινωνιών).[14]

Στη βάση της ανάλυσης που πραγματοποιείται από αυτή τη μελέτη και των συστάσεων που διατυπώνονται σε αυτή, των συμπερασμάτων που αντλούνται από την προαναφερόμενη διαδικασία διαβούλευσης, των νέων δυνατοτήτων που προσφέρονται από τη συνθήκη του Άμστερνταμ και από τις ήδη διεξαγόμενες εργασίες από την Ευρωπαϊκή Ένωση, τις χώρες

βιβλίο για την προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας στις υπηρεσίες του οπτικοακουστικού τομέα και του τομέα πληροφόρησης· COM(96) 483, Οκτώβριος 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm;

Ανακοίνωση της Επιτροπής στο Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή Περιφερειών – Παράνομο και επιζήμιο περιεχόμενο στο Διαδίκτυο (COM(96) 487 τελικό)·

Ψήφισμα για την ανακοίνωση της Επιτροπής για το παράνομο και επιζήμιο περιεχόμενο στο Διαδίκτυο (COM(96) 487 - C4-0592/96)·

Ψήφισμα του Συμβουλίου της 17ης Ιανουαρίου 1995 σχετικά με τη νόμιμη παρακολούθηση των τηλεπικοινωνιών (ΕΕ C 329, 04.11.1996, σ. 1– 6).

11 http://europa.eu.int/comm/justice_home/jai/prog_en.htm.

12 "Legal Aspects of Computer-related Crime in the Information Society – COMCRIME." Η μελέτη πραγματοποιήθηκε από τον καθηγητή U. Sieber του Πανεπιστημίου του Würzburg κατ' εντολή της Ευρωπαϊκής Επιτροπής. Η τελική έκθεση διατίθεται στη διεύθυνση: http://www2.echo.lu/legal/en/crime/crime.html.

13 Στο επίπεδο της Ευρωπαϊκής Ένωσης, οι αρχές ελέγχουν για την προστασία των δεδομένων απαρτίζουν την ομάδα εργασίας για την προστασία των δεδομένων του άρθρου 29, η οποία αποτελεί ανεξάρτητο κοινοτικό όργανο για την προστασία του ιδιωτικού βίου και των δεδομένων, βλέπε άρθρο 29 και 30 της οδηγίας 95/46/ΕΚ.

14 Δύο συνεδριάσεις με τις αρχές εφαρμογής του νόμου έλαβαν χώρα στις 10.12.1999 και στις 1.3.2000, αντίστοιχα. Μια συνεδρίαση με τους αντιπροσώπους των εξειδικευμένων στο Διαδίκτυο επιχειρήσεων έγινε στις 13-3-2000. Ακόμη, μια συνεδρίαση με ένα μικρό αριθμό εμπειρογνωμόνων, όσον αφορά την προστασία των προσωπικών δεδομένων πραγματοποιήθηκε στις 31.3.2000. Η τελική συνεδρίαση με όλους τους παραπάνω αναφερόμενους αντιπροσώπους, έγινε στις 17.4.2000. Αντίγραφα των πρακτικών των συνεδριάσεων μπορούν να χορηγηθούν μετά την αποστολή σχετικής επιστολής στην κάτωθι διεύθυνση: Ευρωπαϊκή Επιτροπή, ΓΔ INFSO Τμήμα Α4, ή στην διεύθυνση: Ευρωπαϊκή Επιτροπή, ΓΔ JAI Τμήμα Β2, οδός Wetstraat/Rue de la Loi 200, 1049 Βρυξέλλες, Βέλγιο.

του G8 και το Συμβούλιο της Ευρώπης, η παρούσα ανακοίνωση θα εξετάσει τις διάφορες δυνατότητες περαιτέρω δράσης της ΕΕ κατά του εγκλήματος πληροφορικής. Στο επίπεδο της Ευρωπαϊκής Ένωσης, οι λύσεις που θα επιλεγούν δεν πρέπει να οδηγήσουν σε παρεμπόδιση και κατακερματισμό της εσωτερικής αγοράς ούτε σε μέτρα που θα υποσκάπτουν την προστασία των θεμελιωδών δικαιωμάτων[15].

2. ΑΣΦΑΛΕΙΑ ΤΩΝ ΥΠΟΔΟΜΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ

Στην κοινωνία της πληροφορίας, τα παγκόσμια δίκτυα που ελέγχονται από το χρήστη τείνουν βαθμιαία να αντικαταστήσουν την παλιά γενιά των εθνικών δικτύων επικοινωνίας. Ένας από τους λόγους που εξηγούν την επιτυχία του Διαδικτύου είναι ότι προσέφερε στους χρήστες πρόσβαση στις πλέον σύγχρονες τεχνολογίες. Ο νόμος του Moore[16] προβλέπει ότι η ηλεκτρονική ισχύς θα διπλασιάζεται ανά 18 μήνες. Εντούτοις οι τεχνολογίες επικοινωνιών σημειώνουν ακόμα πιο γρήγορες προόδους[17]. Μια από τις συνέπειες αυτής της ανάπτυξης είναι ότι ο όγκος των δεδομένων που κυκλοφορεί μέσω του Διαδικτύου διπλασιάζεται σε περιόδους μικρότερες του έτους.

Τα παραδοσιακά τηλεφωνικά δίκτυα κατασκευάζονταν και λειτουργούσαν από εθνικούς οργανισμούς. Οι χρήστες είχαν περιορισμένη επιλογή υπηρεσιών και δεν ασκούσαν έλεγχο όσον αφορά το πλαίσιο. Τα πρώτα δίκτυα δεδομένων που αναπτύχθηκαν στηρίζονταν στην ίδια φιλοσοφία ενός κεντρικά ελεγχόμενου πλαισίου. Η ασφάλεια εντός αυτών των πλαισίων αντικατόπτριζε το γεγονός αυτό.

Το Διαδίκτυο και τα άλλα νέα δίκτυα είναι πολύ διαφορετικά και το θέμα της ασφάλειας χρειάζεται να αντιμετωπιστεί ανάλογα. Σε αυτά τα δίκτυα οι πληροφορίες και ο έλεγχος ευρίσκονται ως επί το πλείστον στην περιφέρεια, εκεί όπου ευρίσκονται οι χρήστες και οι υπηρεσίες. Ο πυρήνας του δικτύου είναι απλός και αποτελεσματικός και έχει ουσιαστικά σαν καθήκον τη διαβίβαση δεδομένων. Υπάρχει περιορισμένος έλεγχος του περιεχομένου. Μόνο στον τελικό προορισμό τα δυαδικά ψηφία (bits) καθίστανται ήχος, εικόνα ή επιβεβαίωση τραπεζικής συναλλαγής. Η ασφάλεια αποτελεί ως εκ τούτου σε μεγάλο βαθμό ευθύνη του χρήστη, δεδομένου ότι μόνο αυτός μπορεί να εκτιμήσει την αξία των δυαδικών ψηφίων (bits) που αποστέλλονται ή λαμβάνονται και μπορεί να καθορίσει το επίπεδο της απαιτούμενης προστασίας.

Το περιβάλλον του χρήστη αποτελεί ως εκ τούτου στοιχείο κλειδί της υποδομής πληροφόρησης. Οι τεχνικές ασφάλειας πρέπει να εφαρμόζονται εκεί με την άδεια και τη συμμετοχή του χρήστη και σύμφωνα με τις ανάγκες του. Αυτό είναι ιδιαίτερα σημαντικό αν λάβει κανείς υπόψη την αυξανόμενη κλίμακα δραστηριοτήτων που μπορούν να διεξαχθούν με βάση τον ίδιο τερματικό. Μπορούμε πράγματι με βάση το ίδιο μηχάνημα, να εργαστούμε, να διασκεδάσουμε, να κοιτάξουμε τηλεόραση και να πραγματοποιήσουμε τραπεζικές πληρωμές.

---

15 Κοινοτικός χάρτης των θεμελιωδών δικαιωμάτων (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), Άρθρο 6 της ΣΕΕ και νομολογία του Ευρωπαϊκού Δικαστηρίου.

16 Αυτή η παρατήρηση διατυπώθηκε το 1965 από τον Gordon Moore, συνιδρυτή της επιχείρησης Intel, επ΄ ευκαιρία του ρυθμού αύξησης του αριθμού τρανζίστορ σε ένα ολοκληρωμένο κύκλωμα. Αυτός ο αριθμός τώρα διπλασιάζεται σχεδόν κάθε 18 μήνες, γεγονός που έχει άμεση επίπτωση στην τιμή και στις αποδόσεις των ηλεκτρονικών τσιπς. Πολλοί εμπειρογνώμονες πιστεύουν ότι αυτός ο νόμος θα συνεχίσει να ισχύει τουλάχιστον για τα δέκα προσεχή έτη.

17 Οι πλέον πρόσφατες τεχνολογίες επιτρέπουν, σε ένα μόνο καλώδιο οπτικών ινών, να διοχετεύεται ταυτόχρονα το ισοδύναμο 100 εκατομμυρίων τηλεφωνικών επικοινωνιών.

Πολλές τεχνολογίες ασφάλειας έχουν ήδη δημιουργηθεί και νέες τεχνολογίες ευρίσκονται υπό ανάπτυξη. Αντιλαμβανόμαστε καλύτερα τα προτερήματα που προσφέρουν τα ανοιχτά λογισμικά από άποψη ασφάλειας. Πολλές εργασίες έχουν διεξαχθεί για την εφαρμογή μεθόδων και κριτηρίων αξιολόγησης της ασφάλειας. Η χρήση των τεχνολογιών κρυπτογράφησης και των ηλεκτρονικών υπογραφών καθίσταται απαραίτητη, ιδιαίτερα ενόψει της ανάπτυξης της ασύρματης πρόσβασης. Χρειαζόμαστε μηχανισμούς απόδειξης της γνησιότητας ολοένα και πιο ποικίλους για να καλυφθούν οι διάφορες ανάγκες μας στο περιβάλλον στο οποίο εξελισσόμεθα. Σε ορισμένα περιβάλλοντα, μπορεί να χρειάζεται ή να επιθυμούμε να παραμείνουμε ανώνυμοι. Σε άλλα, μπορεί να χρειάζεται να μπορεί να αποδειχθεί κάποιο χαρακτηριστικό χωρίς να αποκαλυφθεί η ταυτότητά μας, όπως το γεγονός ότι κάποιος είναι ενήλικος, υπάλληλος ή πελάτης μιας συγκεκριμένης επιχείρησης. Σε άλλες καταστάσεις, τέλος, μπορεί να είναι απαραίτητο να αποδειχθεί η ταυτότητά μας. Επίσης τα φίλτρα λογισμικού καθίστανται ολοένα και πιο πολύπλοκα, γεγονός που μας επιτρέπει να προστατευθούμε, εμείς οι ίδιοι ή τα πρόσωπα που τελούν υπό την επιμέλειά μας, από δεδομένα που δεν επιθυμούμε, όπως το ανεπιθύμητο περιεχόμενο, το ανεπιθύμητο ηλεκτρονικό ταχυδρομείο, κακόβουλα λογισμικά και άλλες μορφές επίθεσης. Η εφαρμογή και διαχείριση τέτοιων αξιώσεων ασφαλείας στο Διαδίκτυο και τα νέα δίκτυα συνεπάγεται σημαντικά έξοδα για τη βιομηχανία και τους χρήστες είναι ως εκ τούτου σημαντικό να ενθαρρυνθεί η καινοτομία και η εμπορική χρήση της τεχνολογίας και των υπηρεσιών ασφαλείας.

Φυσικά, η κοινή υποδομή συνδέσμων επικοινωνίας και εξυπηρετητών ονομάτων θέτει τα δικά της ζητήματα ασφάλειας. Η διαβίβαση δεδομένων εξαρτάται από συνδέσμους μέσω των οποίων τα δεδομένα κατευθύνονται από τον έναν υπολογιστή στον άλλο. Αυτοί οι σύνδεσμοι πρέπει να δημιουργηθούν και να προστατευθούν κατά τρόπο ώστε η διαβίβαση να παραμένει εφικτή παρά τα ατυχήματα, τις επιθέσεις και έναν όγκο κυκλοφορίας συνεχώς αυξανόμενο. Οι επικοινωνίες επίσης εξαρτώνται από υπηρεσίες θεμελιώδους σημασίας όπως εκείνες που παρέχονται από εξυπηρετητές ονομάτων και ειδικότερα από μικρό αριθμό εξυπηρετητών βάσης, οι οποίοι παρέχουν τις απαραίτητες διευθύνσεις. Κάθε ένα από αυτά τα συστατικά θα χρειαστεί επίσης τη δέουσα προστασία, η οποία θα ποικίλει ανάλογα με την αναλογία του χώρου του ονόματος τομέα και του τμήματος πελατείας στην οποία παρέχεται η υπηρεσία.

Επιδιώκοντας να προσφέρει μεγαλύτερη ευελιξία και να ανταποκριθεί στις ανάγκες των ατόμων, η υποδομή των τεχνολογιών πληροφόρησης κατέστη ολοένα και πιο πολύπλοκη καταβάλλοντας συχνά ανεπαρκή προσπάθεια για να καλυφθούν τα θέματα ασφάλειας. Επιπλέον, αυτή η πολυπλοκότητα συνεπάγεται όλο και πιο έντεχνα και διασυνδεδεμένα προγράμματα λογισμικού τα οποία ενίοτε περιλαμβάνουν αδυναμίες και κενά από άποψη ασφάλειας, που μπορούν εύκολα να χρησιμοποιηθούν για επιθέσεις. Όσο ο κυβερνοχώρος γίνεται πιο πολύπλοκος και τα στοιχεία του πιο έντεχνα τόσο μεγαλύτερο είναι το ενδεχόμενο να προκύψουν νέες και απρόβλεπτες αδυναμίες.

Υπάρχουν ήδη διάφορες τεχνικές λύσεις και αναπτύσσονται νέες για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Περιλαμβάνουν μέτρα προκειμένου να :

- εξασφαλισθούν ζωτικά στοιχεία της υποδομής μέσω της ανάπτυξης υποδομών δημόσιων κλειδιών, της ανάπτυξης πρωτοκόλλων ασφάλειας, κλπ.

- εξασφαλισθούν ιδιωτικά και δημόσια περιβάλλοντα μέσω της ανάπτυξης λογισμικών ποιότητας, ζωνών ασφαλείας, προγραμμάτων ανίχνευσης ιών, συστημάτων ηλεκτρονικής διαχείρισης των δικαιωμάτων, κρυπτογράφησης, κλπ.

- εξασφαλισθεί η αναγνώριση των εγκεκριμένων χρηστών, η χρήση έξυπνων καρτών, η βιομετρική αναγνώριση, οι ηλεκτρονικές υπογραφές, οι τεχνικές ελέγχου της πρόσβασης βάσει του ρόλου, κλπ.

Αυτό προϋποθέτει αυξημένη προσπάθεια για την ανάπτυξη τεχνολογιών ασφαλείας καθώς και συνεργασία προκειμένου να επιτευχθεί η απαραίτητη διαλειτουργικότητα μεταξύ των προτεινομένων λύσεων χάρη σε συμφωνίες για διεθνή πρότυπα.

Είναι σημαντικό επίσης να καταστεί κάθε μελλοντικό εννοιολογικό πλαίσιο για την ασφάλεια εγγενές μέρος της συνολικής αρχιτεκτονικής, προβλέποντας λύσεις απέναντι στις απειλές και τις αδυναμίες ήδη κατά την έναρξη της διαδικασίας σχεδιασμού. Αυτό δεν αντιστοιχεί στις παραδοσιακές προσεγγίσεις που επιδιώκουν να αναπτύσσουν επιβοηθητικές λύσεις για την κάλυψη των κενών που εκμεταλλεύονται οι ολοένα και πιο σύνθετες εγκληματικές οργανώσεις που είναι εφοδιασμένες με ολοένα και πιο τελειοποιημένα μέσα.

Το κοινοτικό πρόγραμμα για τις τεχνολογίες της κοινωνίας της πληροφορίας (ΤΚΠ),[18] και κυρίως οι ενέργειες που αφορούν την ασφάλεια των πληροφοριών και των δικτύων και άλλες τεχνολογίες οικοδόμησης εμπιστοσύνης,[19] αποτελεί ένα πλαίσιο για την ανάπτυξη των απαραίτητων ικανοτήτων και τεχνικών προκειμένου να κατανοηθούν και να αντιμετωπιστούν οι προκλήσεις τις οποίες αρχίζει να θέτει το έγκλημα πληροφορικής. Αυτές οι τεχνολογίες συμπεριλαμβάνουν κυρίως τεχνικά εργαλεία προστασίας κατά των προσβολών των θεμελιωδών δικαιωμάτων προστασίας του ιδιωτικού βίου και των προσωπικών δεδομένων, καθώς και άλλων ατομικών δικαιωμάτων, όπως και μέσα καταπολέμησης του εγκλήματος πληροφορικής. Επιπλέον, στο πλαίσιο του προγράμματος ΤΚΠ ξεκίνησε η πρωτοβουλία για την ασφάλεια λειτουργίας. Αυτή η πρωτοβουλία θα συμβάλλει στην οικοδόμηση εμπιστοσύνης στις άκρως διασυνδεδεμένες υποδομές πληροφόρησης και στα στενά ενσωματωμένα δικτυωμένα συστήματα, εντείνοντας την ευαισθητοποίηση όσον αφορά την ασφάλεια λειτουργίας και ενθαρρύνοντας τις τεχνικές που επιτρέπουν να εξασφαλιστεί αυτή η ασφάλεια. Η συνεργασία αποτελεί εγγενές τμήμα αυτής της πρωτοβουλίας. Το πρόγραμμα ΤΚΠ ανέπτυξε σχέσεις εργασίας με την DARPA και την NSF και δημιούργησε, σε συνεργασία με το αμερικανικό υπουργείο εξωτερικών υποθέσεων, μια κοινή Task Force Ευρωπαϊκή Κοινότητα/Ηνωμένες Πολιτείες για την προστασία σημαντικών υποδομών (Joint EC/US Task Force on Critical Infrastructure Protection).[20]

Τέλος, η εφαρμογή των υποχρεώσεων ασφαλείας που προκύπτουν κυρίως από τις οδηγίες της ΕΕ για την προστασία δεδομένων[21] συμβάλλει στην αύξηση της ασφάλειας των δικτύων και της επεξεργασίας δεδομένων.

---

18 Το πρόγραμμα ΤΚΠ διοικείται από την Ευρωπαϊκή Επιτροπή. Αποτελεί τμήμα του 5ου προγράμματος πλαισίου, το οποίο καλύπτει την περίοδο 1998 έως 2002. Για περισσότερες πληροφορίες συμβουλευτείτε τη σελίδα http://www.cordis.lu/ist.

19 Στη δράση κλειδί II - Νέες μέθοδοι εργασίας και ηλεκτρονικό εμπόριο.

20 Υπό την αιγίδα της κοινής συμβουλευτικής ομάδας δυνάμει της συμφωνίας επιστημονικής και τεχνολογικής συνεργασίας μεταξύ της Ευρωπαϊκής Κοινότητας και της κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής.

21 Βλέπε άρθρο 4 της οδηγίας 97/66/ΕΚ (περιλαμβάνει επίσης υποχρέωση ενημέρωσης για τον κίνδυνο παραβίασης της ασφάλειας) και άρθρο 17 της οδηγίας 95/46/ΕΚ.

3. ΕΓΚΛΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τα σύγχρονα συστήματα πληροφόρησης και επικοινωνίας παρέχουν τη δυνατότητα άσκησης παράνομων δραστηριοτήτων οποτεδήποτε και από οποιοδήποτε σημείο του πλανήτη. Δεν υπάρχουν αξιόπιστες στατιστικές που να επιτρέπουν να διαπιστωθεί η πραγματική έκταση του φαινομένου του εγκλήματος πληροφορικής. Ο αριθμός των σφετερισμών που έχουν διαπιστωθεί και επισημανθεί μέχρι σήμερα δεν παρέχει πιθανόν ακριβή ιδέα όσον αφορά όλο το μέγεθος του προβλήματος. Δεδομένου ότι η συνειδητοποίηση και η εμπειρία των διαχειριστών και χρηστών του συστήματος είναι περιορισμένη, πολλές καταχρήσεις δεν έχουν διαπιστωθεί. Επιπλέον, πολλές επιχειρήσεις δεν είναι διατεθειμένες να αναφέρουν περιπτώσεις ηλεκτρονικών καταχρήσεων, για να αποφευχθεί η δυσφήμιση και η έκθεσή τους σε μελλοντικές προσβολές. Οι αστυνομικές υπηρεσίες, στην πλειοψηφία τους, δεν διαθέτουν ακόμα στατιστικές για την χρήση υπολογιστών και συστημάτων επικοινωνίας που ενέχονται σε εγκληματικότητα αυτού του είδους και σε άλλες μορφές εγκληματικότητας. Εντούτοις, πρέπει να αναμένεται η αύξηση του αριθμού παράνομων δραστηριοτήτων στο βαθμό που θα εντατικοποιηθεί η χρήση υπολογιστών και δικτύων. Υπάρχει σαφής ανάγκη να συγκεντρωθούν αξιόπιστα αποδεικτικά στοιχεία για τη σημασία του εγκλήματος πληροφορικής.

Στην παρούσα ανακοίνωση, το έγκλημα πληροφορικής νοείται υπό ευρεία έννοια, για να ορίσει κάθε έγκλημα το οποίο, με τον ένα ή τον άλλο τρόπο, συνεπάγεται τη χρήση τεχνολογίας πληροφοριών. Εντούτοις υπάρχουν διάφορες απόψεις ως προς το τι συνιστά "έγκλημα πληροφορικής". Οι όροι "έγκλημα πληροφορικής", "έγκλημα που διαπράττεται μέσω υπολογιστών", "έγκλημα υψηλής τεχνολογίας" και "έγκλημα στο κυβερνοχώρο" χρησιμοποιούνται συχνά χωρίς διάκριση. Μπορεί να γίνει διάκριση μεταξύ ειδικών εγκλημάτων πληροφορικής και παραδοσιακών εγκλημάτων που διαπράττονται με τη βοήθεια της τεχνολογίας των ηλεκτρονικών υπολογιστών. Ένα επίκαιρο παράδειγμα που καταδεικνύει αυτήν τη διάκριση αφορά τα τελωνεία, όπου το Διαδίκτυο αποδεικνύεται ότι αποτελεί μέσο για τη διάπραξη παραδοσιακών παραβάσεων της τελωνειακής νομοθεσίας, όπως το λαθρεμπόριο, η παραποίηση κλπ. Ενώ τα εγκλήματα πληροφορικής απαιτούν ενημέρωση των ορισμών των εγκλημάτων στους εθνικούς ποινικούς κώδικες, τα παραδοσιακά εγκλήματα που διαπράττονται με τη βοήθεια ηλεκτρονικών υπολογιστών επιβάλουν τη βελτίωση της συνεργασίας και τη θέσπιση διαδικαστικών μέτρων.

Όλα αυτά τα εγκλήματα έχουν εντούτοις σαν κοινά χαρακτηριστικά την εκμετάλλευση των υφιστάμενων δικτύων πληροφόρησης και επικοινωνίας, τα οποία δεν γνωρίζουν σύνορα, και την κυκλοφορία δεδομένων η οποία είναι άυλη και άκρως ευμετάβλητη. Αυτά τα χαρακτηριστικά απαιτούν την αναθεώρηση των υφιστάμενων μέτρων για να αντιμετωπιστούν παράνομες δραστηριότητες που εκτελούνται σε ή με αυτά τα δίκτυα και συστήματα.

Πολλές χώρες έχουν θεσπίσει νομοθεσία για το έγκλημα πληροφορικής. Στα κράτη μέλη της Ευρωπαϊκής Ένωσης έχει θεσπιστεί σειρά νομικών μέσων. Πέραν της απόφασης του Συμβουλίου για την παιδική πορνογραφία στο Διαδίκτυο, ακόμα και αν δεν διαθέτουμε μέχρι σήμερα κανένα κοινοτικό νομικό μέσο το οποίο να ασχολείται άμεσα με το έγκλημα πληροφορικής, υπάρχουν ορισμένα νομικά μέσα που ισχύουν έμμεσα.

Τα κύρια προβλήματα με τα οποία ασχολείται η υπάρχουσα νομοθεσία στον τομέα των εγκλημάτων πληροφορικής, τόσο στο επίπεδο της Ευρωπαϊκής Ένωσης όσο και στο επίπεδο των κρατών μελών, είναι τα ακόλουθα:

Προσβολές του ιδιωτικού βίου: Πολλά κράτη έχουν θεσπίσει ποινική νομοθεσία σχετικά με την παράνομη συλλογή, αποθήκευση, τροποποίηση, γνωστοποίηση και διάδοση των δεδομένων προσωπικού χαρακτήρα. Στο επίπεδο της Ευρωπαϊκής Ένωσης, υπάρχουν δυο οδηγίες οι οποίες προσεγγίζουν τις εθνικές νομοθεσίες για την προστασία του ιδιωτικού βίου στο πλαίσιο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.[22] Το άρθρο 24 της οδηγίας 95/46/ΕΚ υποχρεώνει σαφώς τα κράτη μέλη να λαμβάνουν τα κατάλληλα μέτρα για να εξασφαλίσουν την πλήρη εφαρμογή των διατάξεων της οδηγίας , συμπεριλαμβανομένων κυρώσεων για παράβαση των διατάξεων εφαρμογής της. Τα θεμελιώδη δικαιώματα προστασίας του ιδιωτικού βίου και προστασίας των δεδομένων περιλαμβάνονται επιπλέον στο χάρτη των θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Παραβάσεις που έχουν σχέση με το περιεχόμενο: η διάδοση, ιδιαίτερα στο Διαδίκτυο, πορνογραφικών εικόνων, ρατσιστικών διακηρύξεων και πληροφοριών που παροτρύνουν σε βία θέτει το ζήτημα του κατά πόσον αυτές οι πράξεις μπορούν να αντιμετωπιστούν με τη βοήθεια του ποινικού δικαίου. Η Επιτροπή υποστήριξε την άποψη ότι αυτό που θεωρείται παράνομο εκτός σύνδεσης (off-line) πρέπει να θεωρείται εξίσου παράνομο σε απευθείας σύνδεση (on-line). Ο δημιουργός ή ο φορέας παροχής περιεχομένου[23] μπορεί να θεωρείται υπεύθυνος σύμφωνα με το ποινικό δίκαιο. Θεσπίστηκε απόφαση του Συμβουλίου για να καταπολεμηθεί η παιδική πορνογραφία στο Διαδίκτυο.[24]

Η ευθύνη των ενδιάμεσων φορέων παροχής υπηρεσιών, των οποίων τα δίκτυα ή οι εξυπηρετητές χρησιμοποιούνται για τη διαβίβαση ή την αποθήκευση πληροφοριών σε τρίτους, προβλέπεται από την οδηγία για το ηλεκτρονικό εμπόριο.

Οικονομικά εγκλήματα, μη εγκεκριμένη πρόσβαση και δολιοφθορά: Πολλά κράτη έχουν θεσπίσει νομοθεσία για το οικονομικό έγκλημα πληροφορικής, η οποία καθορίζει νέα αδικήματα που συνδέονται με την μη εγκεκριμένη πρόσβαση στα ηλεκτρονικά συστήματα (για παράδειγμα, ηλεκτρονική πειρατεία, ηλεκτρονική δολιοφθορά και διάδοση ιών, ηλεκτρονική κατασκοπεία, ηλεκτρονική πλαστογραφία ή απάτη[25]) και νέες μορφές διάπραξης αδικημάτων (για παράδειγμα, ηλεκτρονική πλαστογράφηση αντί της παραπλάνησης φυσικού προσώπου). Ο στόχος του εγκλήματος είναι συχνά άϋλος, π.χ. χρήματα σε τραπεζικούς λογαριασμούς ή ηλεκτρονικά προγράμματα. Επί του παρόντος δεν

---

22 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία αυτών των δεδομένων και οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15 Δεκεμβρίου 1997 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία του ιδιωτικού βίου στον τομέα των τηλεπικοινωνιών. Το άρθρο 24 της οδηγίας 95/46/ΕΚ αναθέτει την υποχρέωση στα κράτη μέλη να καθορίζουν τις κυρώσεις που πρέπει να εφαρμόζονται σε περιπτώσεις παράβασης των διατάξεων που αφορούν την προστασία των δεδομένων.

23 Ο φορέας παροχής περιεχομένου δεν πρέπει να συγχέεται με τον φορέα παροχής υπηρεσιών.

24 Απόφαση του Συμβουλίου της 29ης Μαΐου 2000 σχετικά με την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο (ΕΕ L 138, της 9.6.2000, σ.1).

25 Τα μαζικά μέσα ενημέρωσης έχουν δώσει μεγάλη προσοχή στις πρόσφατες επιθέσεις "άρνησης παροχής υπηρεσίας" στις μεγάλες διευθύνσεις του Διαδικτύου και στη διάδοση του ιού που φέρει την ονομασία LoveBug. Πρέπει εντούτοις να σχετικοποιήσουμε την επικαιρότητα του προβλήματος. Οι επιθέσεις άρνησης υπηρεσίας, σκόπιμες ή απροσχεδίαστες, καθώς και η διάδοση ιών με το ηλεκτρονικό ταχυδρομείο εμφανίστηκαν εδώ και πολλά έτη. Ο ιός Morris και ο ιός του χριστουγεννιάτικου δέντρου (IBM Xmas-tree) υπήρξαν τα πρώτα παραδείγματα. Υπάρχουν προϊόντα και διαδικασίες για να αντιμετωπιστούν αυτοί οι ιοί. Υπάρχει επίσης καλό πνεύμα συνεργασίας μεταξύ των χρηστών του Διαδικτύου για να περιοριστούν οι ζημιές που μπορούν να προξενηθούν από τέτοια περιστατικά. Υπάρχει παρόμοια συνεργασία για να περιοριστούν οι καταχρήσεις που έχουν σχέση με τη διάδοση μη ζητηθέντων μηνυμάτων.

υπάρχουν κοινοτικά νομικά μέτρα που να ασχολούνται με αυτού του είδους τις παράνομες δραστηριότητες. Όσον αφορά την πρόληψη, ο πρόσφατα εγκριθείς αναθεωρημένος κανονισμός για τα αγαθά διπλής χρήσης συνέβαλε σημαντικά στην απελευθέρωση της διαθεσιμότητας προϊόντων κρυπτογράφησης.

Προσβολές της πνευματικής ιδιοκτησίας: Έχουν εκδοθεί δυο οδηγίες σχετικά με τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών και των βάσεων δεδομένων,[26] οι οποίες αφορούν άμεσα την κοινωνία της πληροφορίας και προβλέπουν κυρώσεις. Το Συμβούλιο εξέδωσε κοινή θέση για πρόταση σχετικά με την πνευματική ιδιοκτησία και τα συγγενικά δικαιώματα στην κοινωνία της πληροφορίας. Αυτή η οδηγία πρόκειται να εγκριθεί κατά τις αρχές του 2001[27]. Η παράβαση των δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων καθώς και η εξουδετέρωση των εθνικών μέσων που έχουν τεθεί σε εφαρμογή για την προστασία αυτών των δικαιωμάτων πρέπει να τιμωρούνται. Όσον αφορά την πλαστογραφία και την πειρατεία, η Επιτροπή θα υποβάλει πριν από τα τέλη του 2000 ανακοίνωση με την οποία θα κάνει απολογισμό της διαδικασίας διαβούλευσης που ξεκίνησε με το Πράσινο Βιβλίο του 1998 και θα αναγγείλει σχέδιο δράσης στο συγκεκριμένο τομέα. Στο βαθμό που το Διαδίκτυο αποκτά ολοένα και μεγαλύτερη σημασία σε εμπορικό επίπεδο, αρχίζουν να διαφαίνονται νέες διαφορές όσον αφορά τα ονόματα τομέα που αφορούν το cybersquatting (κατάληψη του κυβερνοχώρου), warehousing (καταχρηστική εναποθήκευση) και reverse hijacking (πειρατεία) και, φυσικά, υπάρχει και στο προκείμενο ανάγκη κανόνων και διαδικασιών για την αντιμετώπιση αυτών των προβλημάτων.[28]

Πρέπει επίσης να τεθεί το ζήτημα της τήρησης των φορολογικών υποχρεώσεων. Στις εμπορικές συναλλαγές στις οποίες ο αποδέκτης παροχής ηλεκτρονικής υπηρεσίας σε απευθείας σύνδεση (on-line) ευρίσκεται στην Ευρωπαϊκή Ένωση, η φορολογική υποχρέωση γεννάται, στις περισσότερες των περιπτώσεων, στο έδαφος στο οποίο θεωρείται ότι λαμβάνει χώρα η κατανάλωση αυτών των υπηρεσιών[29]. Η παράλειψη συμμόρφωσης με τις φορολογικές υποχρεώσεις της εκθέτει την επιχείρηση σε αστικές κυρώσεις (ή ποινικές σε ορισμένες περιπτώσεις), οι οποίες μπορούν να συμπεριλάβουν την κατάσχεση τραπεζικών λογαριασμών ή άλλων περιουσιακών στοιχείων. Παρά το γεγονός ότι η εθελουσία συμμόρφωση αποτελεί την προτιμότερη λύση, αυτές οι υποχρεώσεις πρέπει σε τελευταία ανάλυση να είναι εκτελεστές. Η συνεργασία μεταξύ των φορολογικών διοικήσεων αποτελεί βασικό στοιχείο για την επίτευξη αυτού του στόχου.

---

[26] Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών (ΕΕ L 122 , 17.5.1991, σ. 42 – 46).
Οδηγία 96/9/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαρτίου 1996 για τη νομική προστασία των βάσεων δεδομένων (ΕΕ L 77, της 27.3.1996, σ. 20 – 28).

[27] Κοινή θέση που υιοθετήθηκε από το Συμβούλιο, εν όψει της υιοθέτησης της Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με την εναρμόνιση ορισμένων θεμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων στην Κοινωνία των Πληροφοριών (CS/2000/9512).

[28] Ανακοίνωση της Επιτροπής στο Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, - Η Οργάνωση και Διαχείριση του Διαδικτύου, - Ζητήματα Διεθνούς και Ευρωπαϊκής Πολιτικής 1998-2000, Απρίλιος 2000, COM(2000) 202.

[29] Η Επιτροπή πρότεινε σειρά τροποποιήσεων του κοινοτικού συστήματος ΦΠΑ, που αποσκοπούν να διευκρινήσουν τον τόπο φορολογίας (COM(2000)349 - Πρόταση οδηγίας του Συμβουλίου γα την τροποποίηση της οδηγίας 77/388/ΕΟΚ σχετικά με το σύστημα φόρου προστιθέμενης αξίας που εφαρμόζεται σε ορισμένες υπηρεσίες παρεχόμενες με ηλεκτρονικά μέσα), η οποία εξετάζεται επί του παρόντος στο Συμβούλιο και το Κοινοβούλιο. Σε ορισμένες περιπτώσεις εντούτοις η φορολογική υποχρέωση μπορεί να βαρύνει τον προμηθευτή, ακόμα και αν αυτός δεν είναι φυσικά παρών στον τόπο της φορολογικής δικαιοδοσίας.

Η δυνατότητα που παρέχεται σε ορισμένους να προστατεύουν τις νόμιμες συναλλαγές του παρέχει εξίσου τα ίδια μέσα σε εγκληματίες ώστε να προστατεύουν τις παράνομες συναλλαγές τους. Τα εργαλεία που μας παρέχουν ασφαλές ηλεκτρονικό εμπόριο μπορούν εξίσου να χρησιμοποιηθούν για το λαθρεμπόριο ναρκωτικών. Πρέπει να καθορισθούν οι προτεραιότητες και να γίνουν επιλογές.

Η προστασία των θυμάτων του εγκλήματος πληροφορικής χρειάζεται επίσης να καλύψει θέματα ευθύνης, αποκατάστασης και αποζημίωσης που τίθενται στο πλαίσιο των εγκλημάτων πληροφορικής. Η εμπιστοσύνη εξαρτάται όχι μόνο από τη χρήση των κατάλληλων τεχνικών αλλά εξίσου από τις παρεχόμενες νομικές και οικονομικές εγγυήσεις. Αυτά τα θέματα θα πρέπει να εξετασθούν για όλες τις μορφές εγκλημάτων πληροφορικής.

Υπάρχει ανάγκη για αποτελεσματικά εναρμονισμένα νομικά και δικονομικά μέσα, αν όχι σε παγκόσμιο επίπεδο, τουλάχιστον σε ευρωπαϊκό επίπεδο, προκειμένου να προστατευθούν τα θύματα του εγκλήματος πληροφορικής και να διωχθούν οι δράστες αυτών των παραβάσεων. Παράλληλα, οι ανακοινώσεις προσωπικού χαρακτήρα, η προστασία του ιδιωτικού βίου και των δεδομένων, η πρόσβαση στην πληροφόρηση και η διάδοσή της αποτελούν θεμελιώδη δικαιώματα των σύγχρονων δημοκρατιών. Αυτός είναι ο λόγος για τον οποίο θα πρέπει να υπάρχουν και να χρησιμοποιούνται αποτελεσματικά μέτρα πρόληψης κατά τρόπο ώστε να καθίστανται λιγότερο απαραίτητα τα κατασταλτικά μέτρα. Οποιοδήποτε νομοθετικό μέτρο αποδειχθεί απαραίτητο για την καταπολέμηση του εγκλήματος πληροφορικής θα πρέπει να βρει τη σωστή ισορροπία μεταξύ αυτών των σημαντικών συμφερόντων.

4. ΖΗΤΗΜΑΤΑ ΟΥΣΙΑΣΤΙΚΟΥ ΔΙΚΑΙΟΥ

Η προσέγγιση των διατάξεων ουσιαστικού δικαίου στον τομέα του εγκλήματος υψηλής τεχνολογίας θα εξασφαλίσει ένα ελάχιστο επίπεδο προστασίας στα θύματα του εγκλήματος πληροφορικής (για παράδειγμα, θύματα της παιδικής πορνογραφίας), θα βοηθήσει στην εκπλήρωση της αξίωσης σύμφωνα με την οποία μια δραστηριότητα πρέπει να αποτελεί αδίκημα και στις δυο ενδιαφερόμενες χώρες πριν να μπορεί να παρασχεθεί αμοιβαία δικαστική συνδρομή στο πλαίσιο ποινικής έρευνας (αξίωση του διπλού αξιόποινου), και θα διευκρινίσει την κατάσταση για τις επιχειρήσεις (για παράδειγμα, σχετικά με αυτό που συνιστά παράνομο περιεχόμενο).

Πράγματι, η θέσπιση κοινοτικού νομοθετικού μέσου που να προσεγγίζει το ποινικό δίκαιο στον τομέα του εγκλήματος πληροφορικής συγκαταλέγεται μεταξύ των προτεραιοτήτων της Ευρωπαϊκής Ένωσης ήδη από το Ευρωπαϊκό Συμβούλιο του Τάμπερε τον Οκτώβριο του 1999[30]. Αυτό το Συμβούλιο συμπεριέλαβε το έγκλημα υψηλής τεχνολογίας σε περιορισμένο κατάλογο τομέων στους οποίους πρέπει να καταβληθούν προσπάθειες για να επιτευχθεί συμφωνία για κοινούς ορισμούς, ποινική πρόβλεψη και κυρώσεις. Αυτό περιλαμβάνεται επίσης στη σύσταση αριθ. 7 για τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και καταστολή του οργανωμένου εγκλήματος για τη νέα χιλιετία, που θεσπίστηκε από το Συμβούλιο ΔΕΥ το Μάρτιο 2000[31]. Εγγράφεται επίσης στο πρόγραμμα εργασίας της Επιτροπής για το έτος 2000 καθώς και στον πίνακα αποτελεσμάτων για τη

---

30 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

31 Πρόληψη και έλεγχος του οργανωμένου εγκλήματος. Στρατηγική της Ευρωπαϊκής Ένωσης για την αρχή της νέας χιλιετίας (ΕΕ C 124, 3.5.2000).

δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, που υποβλήθηκε από την Επιτροπή και εγκρίθηκε από το Συμβούλιο "ΔΕΥ" στις 27 Μαρτίου 2000[32].

Η Επιτροπή παρακολούθησε τις εργασίες του Συμβουλίου της Ευρώπης που αφορούν τη σύμβαση για το έγκλημα στον κυβερνοχώρο. Αυτό το σχέδιο σύμβασης, αναφέρει, υπό την παρούσα εκδοχή του, τέσσερις κατηγορίες ποινικών αδικημάτων: 1) εγκλήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας ηλεκτρονικών δεδομένων και συστημάτων· 2) εγκλήματα πληροφορικής 3) εγκλήματα που αφορούν το περιεχόμενο και 4) εγκλήματα που αφορούν προσβολές της πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων.

Η προσέγγιση σε κοινοτικό επίπεδο θα μπορούσε να είναι πιο προωθημένη από τη σύμβαση του Συμβουλίου της Ευρώπης, η οποία αντιπροσωπεύει μια ελάχιστη διεθνή προσέγγιση. Θα μπορούσε να είναι λειτουργική σε μικρότερο χρονικό διάστημα από ότι χρειάζεται για να τεθεί σε ισχύ η σύμβαση του Συμβουλίου της Ευρώπης.[33] Θα ενσωμάτωνε το έγκλημα πληροφορικής στο πεδίο εφαρμογής του κοινοτικού δικαίου και θα δημιουργούσε κοινοτικούς μηχανισμούς εφαρμογής.

Η Επιτροπή προσδίδει μεγάλη σημασία στο να εξασφαλίσει ότι η Ευρωπαϊκή Ένωση θα είναι σε θέση να αναλάβει αποτελεσματική δράση ιδιαίτερα κατά της παιδικής πορνογραφίας στο Διαδίκτυο. Η Επιτροπή καλωσορίζει την απόφαση του Συμβουλίου για την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο, αλλά συμμερίζεται την άποψη του Ευρωπαϊκού Κοινοβουλίου ότι απαιτείται περαιτέρω δράση για την προσέγγιση των εθνικών νομοθεσιών. Η Επιτροπή προτίθεται να υποβάλει πριν από το τέλος αυτού του έτους πρόταση απόφασης - πλαισίου του Συμβουλίου η οποία θα περιλαμβάνει διατάξεις για την προσέγγιση των νομοθεσιών και των κυρώσεων που αφορούν την παιδική πορνογραφία στο Διαδίκτυο.[34]

Σύμφωνα με τα συμπεράσματα του Τάμπερε, η Επιτροπή θα υποβάλει νομοθετική πρόταση βάσει του τίτλου IV της συνθήκης για την Ευρωπαϊκή Ένωση προκειμένου να προσεγγίσει τις εθνικές διατάξεις που αφορούν το έγκλημα υψηλής τεχνολογίας. Αυτή η πρόταση θα λάβει υπόψη τις προόδους των διαπραγματεύσεων στο πλαίσιο του Συμβουλίου της Ευρώπης και θα εξετάσει ειδικότερα την ανάγκη προσέγγισης των νομοθεσιών που αφορούν την ηλεκτρονική πειρατεία και τις επιθέσεις μέσω της άρνησης υπηρεσίας. Αυτή η πρόταση θα περιλαμβάνει πρότυπους ορισμούς για την Ευρωπαϊκή Ένωση στο συγκεκριμένο τομέα. Θα μπορούσε εξίσου να υπερβεί το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης κατοχυρώνοντας ότι οι σοβαρές περιπτώσεις πειρατείας και επιθέσεων μέσω άρνησης υπηρεσίας θα τιμωρούνται με μία ελάχιστη ποινή σε όλα τα κράτη μέλη.

Περαιτέρω, η Επιτροπή θα εξετάσει τις δυνατότητες δράσης κατά του ρατσισμού και της ξενοφοβίας στο Διαδίκτυο με σκοπό να υποβάλει πρόταση απόφασης-πλαισίου του Συμβουλίου σύμφωνα με τον τίτλο VI της ΣΕΕ, που να καλύπτει τις δραστηριότητες ρατσισμού και ξενοφοβίας τόσο off-line όσο και on-line. Αυτή η πρόταση θα λάβει υπόψη τα

---

32 http://europa.eu.int/comm/dgs/justice_home/index_en.htm.

33 Η σύμβαση του Συμβουλίου της Ευρώπης μπορεί να τεθεί σε ισχύ μόνο μετά την επικύρωσή της.

34 Αυτή η πρωτοβουλία αποτελεί μέρος ενός συνόλου προτάσεων που καλύπτουν εξίσου ευρύτερα θέματα που συνδέονται με τη σεξουαλική εκμετάλλευση των παιδιών και την εμπορία ανθρώπων, όπως είχε ανακοινώσει η Επιτροπή στην ανακοίνωσή της του Δεκεμβρίου 1998 για την εμπορία ανθρώπων. Το κείμενο της πρότασης απόφασης-πλαισίου του Συμβουλίου προσαρτάται στην ανακοίνωση της Επιτροπής στο Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο για την καταπολέμηση της εμπορίας ανθρώπων και της σεξουαλικής εκμετάλλευσης παιδιών - δυο προτάσεις αποφάσεων - πλαισίων που δημοσιεύονται παράλληλα με τη συγκεκριμένη ανακοίνωση.

αποτελέσματα της προσεχούς αξιολόγησης της εφαρμογής από τα κράτη μέλη της κοινής δράσης της 15ης Ιουλίου 1996 για την καταπολέμηση του ρατσισμού και της ξενοφοβίας[35]. Αυτή η κοινή δράση αποτέλεσε ένα πρώτο βήμα προς την κατεύθυνση της προσέγγισης των ποινικών αδικημάτων που έχουν σχέση με το ρατσισμό και την προσέγγιση στο εσωτερικό της Ευρωπαϊκής Ένωσης. Η σημασία και ο ευαίσθητος χαρακτήρας αυτών των φαινομένων τονίσθηκαν στην απόφαση ενός γαλλικού δικαστηρίου της 20ης Νοεμβρίου 2000 η οποία επέβαλε την αξίωση στο Yahoo να παρεμποδίζει την πρόσβαση των γάλλων χρηστών σε ιστοσελίδες που πωλούσαν αντικείμενα της ναζιστικής περιόδου[36].

Τέλος, η Επιτροπή θα εξετάσει τις δυνατότητες βελτίωσης της αποτελεσματικότητας των προσπαθειών καταπολέμησης του εμπορίου παράνομων ναρκωτικών ουσιών στο Διαδίκτυο, της οποίας η σημασία αναγνωρίστηκε στην στρατηγική κατά των ναρκωτικών της Ευρωπαϊκής Ένωσης (2000-2004) η οποία αποφασίστηκε στο Ευρωπαϊκό Συμβούλιο του Ελσίνκι[37].

5. ΖΗΤΗΜΑΤΑ ΔΙΚΟΝΟΜΙΚΟΥ ΔΙΚΑΙΟΥ

Ο ίδιος ο χαρακτήρας των εγκλημάτων πληροφορικής επισύρει την εθνική και διεθνή προσοχή στα θέματα διαδικασίας στο μέτρο που συγκρούονται διάφορες εθνικές κυριαρχίες, δικαιοδοσίες και νομοθεσίες. Περισσότερο από κάθε άλλη μορφή διεθνούς εγκληματικότητας, η ταχύτητα, η κινητικότητα και η ευελιξία του εγκλήματος πληροφορικής θέτει υπό αμφισβήτηση τους ισχύοντες κανόνες ποινικής δικονομίας.

Η προσέγγιση των εξουσιών στον τομέα του δικονομικού δικαίου θα βελτιώσει την προστασία των θυμάτων κατοχυρώνοντας ότι οι υπηρεσίες εφαρμογής του νόμου θα διαθέτουν τις εξουσίες που χρειάζονται για την διερεύνηση εγκλημάτων που διαπράττονται στην επικράτειά τους και θα είναι σε θέση να ανταποκρίνονται με ταχύτητα και αποτελεσματικότητα στις αιτήσεις συνεργασίας άλλων χωρών.

Είναι επίσης σημαντικό να εξασφαλιστεί ότι τα μέτρα που λαμβάνονται στη βάση του ποινικού δικαίου, το οποίο υπάγεται γενικά στη δικαιοδοσία των κρατών μελών και στη βάση του Τίτλου VI της ΣΕΕ συμφωνούν με τις αξιώσεις του κοινοτικού δικαίου. Ιδιαίτερα, το Δικαστήριο έχει επανειλημμένα υποστηρίξει ότι αυτές οι νομοθετικές διατάξεις δεν πρέπει να εισάγουν διακρίσεις εις βάρος ατόμων στα οποία το κοινοτικό δίκαιο παρέχει το δικαίωμα ίσης μεταχείρισης ούτε να περιορίζουν τις θεμελιώδεις ελευθερίες που κατοχυρώνονται από το κοινοτικό δίκαιο[38]. Κάθε νέα εξουσία για την εφαρμογή του νόμου χρειάζεται να αξιολογείται σε σχέση με το κοινοτικό δίκαιο και με τις επιπτώσεις τις οποίες έχει στο δικαίωμα προστασίας του ιδιωτικού βίου.

---

35 ΕΕ L 185, 24/07/1996, σ. 5-7. Διατίθεται επίσης στην διεύθυνση του Ευρωπαϊκού Δικαστικού Δικτύου http://ue.eu.int/ejn/index.htm.

36 Tribunal De Grande Instance de Paris, απόφαση ασφαλιστικών μέτρων που εξεδόθη στις 20 Νοεμβρίου 2000, αριθ. RG 00/05308.

37 Σχέδιο δράσης της Ευρωπαϊκής Ένωσης για την καταπολέμηση των ναρκωτικών (2000–2004). COM(1999) 239 τελικό. http://europa.eu.int/comm/justice_home/unit/drogue_en.htm.

38 Υπόθεση C-274/96 Bickel & Franz (1998) Συλλογή I-7637 παράγραφος 17, Υπόθεση C-186/87 Cowan (1989) Συλλογή 195 παράγραφος 19. Ειδικότερα, τα διοικητικά μέτρα ή κυρώσεις δεν πρέπει να υπερβαίνουν το απολύτως αναγκαίο, οι διαδικασίες ελέγχου δεν πρέπει να εφαρμόζονται κατά τρόπο που να περιορίζεται η ελευθερία που αξιώνεται από τη Συνθήκη και δεν πρέπει να συνοδεύονται από ποινή τόσο δυσανάλογη προς τη βαρύτητα της παράβασης που να αποτελούν εμπόδια για την άσκηση αυτής της ελευθερίας (Υπόθεση C-203/80 Casati (1981) Συλλογή 2595 παράγραφος 27).

5.1. Παρακολούθηση επικοινωνιών

Στην Ευρωπαϊκή Ένωση υπάρχει η γενική αρχή της εμπιστευτικότητας των συνδιαλέξεων (και των σχετικών δεδομένων κίνησης). Η παρακολούθηση είναι παράνομη εκτός εάν επιτρέπεται από το νόμο όταν χρειάζεται σε ειδικές περιπτώσεις και για περιορισμένους σκοπούς. Αυτό προκύπτει από το άρθρο 8 της Ευρωπαϊκής Σύμβασης Ανθρωπίνων Δικαιωμάτων, που αναφέρεται στο άρθρο 6 της ΣΕΕ, και ειδικότερα από τις οδηγίες 95/46/ΕΚ και 97/66/ΕΚ.

Όλα τα κράτη μέλη έχουν θέσει σε λειτουργία ένα νομικό πλαίσιο που επιτρέπει στις υπηρεσίες δίωξης να λαμβάνουν δικαστικό ένταλμα (ή στην περίπτωση δύο κρατών μελών εξουσιοδότηση που παρέχεται προσωπικά από υπουργό που κατέχει υψηλή θέση στην υπουργική ιεραρχία) για την παρακολούθηση συνδιαλέξεων στο δημόσιο δίκτυο τηλεπικοινωνιών.[39] Αυτή η νομοθεσία που πρέπει να συμφωνεί με το κοινοτικό δίκαιο στο βαθμό που αυτό εφαρμόζεται, προβλέπει εγγυήσεις για την προστασία του ιδιωτικού βίου των ατόμων, περιορίζοντας για παράδειγμα την παρακολούθηση συνδιαλέξεων σε περιπτώσεις έρευνας σοβαρών εγκλημάτων και επιβάλλοντας την αξίωση η παρακολούθηση συνδιαλέξεων σε ατομικές έρευνες να είναι απαραίτητη και αναλογική ή εξασφαλίζοντας ότι το άτομο θα ενημερώνεται για την παρακολούθηση μόλις αυτό δεν εμποδίζει την καλή διεξαγωγή της έρευνας. Σε πολλά κράτη μέλη, η νομοθεσία που αφορά την παρακολούθηση συνδιαλέξεων προβλέπει την υποχρέωση των επιχειρήσεων τηλεπικοινωνιών (που εξασφαλίζουν δημόσια υπηρεσία) να εξασφαλίζουν δυνατότητες παρακολούθησης των συνδιαλέξεων. Ένα ψήφισμα του Συμβουλίου του 1995 προβλέπει το συντονισμό των αξιώσεων νόμιμης παρακολούθησης των τηλεπικοινωνιών.[40]

Οι φορείς των παραδοσιακών δικτύων, ιδιαίτερα εκείνοι που παρέχουν υπηρεσίες φωνητικής τηλεφωνίας, έχουν ήδη κατά το παρελθόν συνάψει σχέσεις εργασίας με τις αρχές εφαρμογής του νόμου προκειμένου να διευκολύνουν τη νόμιμη παρακολούθηση των τηλεπικοινωνιών. Η ελευθέρωση των τηλεπικοινωνιών και η ραγδαία ανάπτυξη του Διαδικτύου προσήλκυσαν πολλές νέες επιχειρήσεις στην αγορά, στις οποίες επεβλήθησαν εκ νέου υποχρεώσεις όσον αφορά τη νόμιμη παρακολούθηση. Θα πρέπει να συζητηθούν, στο πλαίσιο του διαλόγου μεταξύ των δημοσίων αρχών και των επιχειρήσεων καθώς και όλων των άλλων ενδιαφερομένων, περιλαμβανομένων των αρχών εποπτείας της προστασίας των προσωπικών

---

39 Δύο κράτη μέλη δεν αναγνωρίζουν την παρακολούθηση συνδιαλέξεων ως αποδεικτικό στοιχείο στις ποινικές διαδικασίες.

40 Ψήφισμα του Συμβουλίου της 17ης Ιανουαρίου 1995 σχετικά με τη νόμιμη παρακολούθηση των τηλεπικοινωνιών (ΕΕ C 329, 4.11.1996, σ. 1– 6). Το παράρτημα περιέχει κατάλογο των απαιτήσεων των νομίμως εξουσιοδοτημένων αρχών όσον αφορά τη νόμιμη παρακολούθηση τηλεπικοινωνιών τις οποίες τα κράτη μέλη καλούνται να λάβουν υπόψη κατά τον καθορισμό και την εφαρμογή των σχετικών εθνικών πολιτικών και μέτρων. Το 1998, η αυστριακή προεδρία πρότεινε ένα ψήφισμα του Συμβουλίου της Ευρωπαϊκής Ένωσης με σκοπό να προεκτείνει το πεδίο εφαρμογής του ψηφίσματος του 1995 στις νέες τεχνολογίες, κυρίως το Διαδίκτυο και τις επικοινωνίες μέσω δορυφόρου. Αυτό το θέμα αποτέλεσε το αντικείμενο συζήτησης στο πλαίσιο δυο επιτροπών του Ευρωπαϊκού Κοινοβουλίου, της επιτροπής πολιτικών ελευθεριών και εσωτερικών υποθέσεων και της επιτροπής νομικών θεμάτων και δικαιωμάτων των πολιτών, οι οποίες κατέληξαν σε διαφορετικά συμπεράσματα. Η πρώτη θεώρησε πράγματι αυτό το ψήφισμα ως διευκρίνηση και ενημέρωση του παλαιού ψηφίσματος και το έκρινε αποδεκτό. Η δεύτερη αντιθέτως, διατύπωσε έντονες κριτικές, τόσο ως προς τις δυνάμει προσβολές των ατομικών δικαιωμάτων όσο και προς το οικονομικό κόστος που συνεπάγεται για τους φορείς, γεγονός που την οδήγησε να απορρίψει την πρόταση του Συμβουλίου και να καλέσει την Επιτροπή να επεξεργαστεί νέα πρόταση μετά την έναρξη ισχύος της συνθήκης του Άμστερνταμ. Το σχέδιο ψηφίσματος του Συμβουλίου δεν έχει αποτελέσει το αντικείμενο εμπεριστατωμένης εξέτασης από το Συμβούλιο ή από τις ομάδες εργασίας του Συμβουλίου κατά τους τελευταίους μήνες.

δεδομένων θέματα που άπτονται της νομοθεσίας, της τεχνικής σκοπιμότητας, της κατανομής του κόστους και της εμπορικής επίπτωσης.

Οι νέες τεχνολογίες καθιστούν απαραίτητη τη συνεργασία μεταξύ των κρατών μελών εφόσον επιθυμούν να διατηρήσουν τη δυνατότητα να παρακολουθούν νομίμως τις συνδιαλέξεις. Η Επιτροπή θεωρεί ότι, αν τα κράτη μέλη επιβάλουν στις επιχειρήσεις τηλεπικοινωνιών και στους παρέχοντες υπηρεσίες στο Διαδίκτυο νέες τεχνικές υποχρεώσεις όσον αφορά την παρακολούθηση, αυτοί οι κανόνες θα πρέπει να αποτελέσουν το αντικείμενο διεθνούς συντονισμού προκειμένου να αποφευχθεί η νόθευση της εσωτερικής αγοράς, να μειωθεί στο ελάχιστο το κόστος το οποίο θα βαρύνει τις επιχειρήσεις και να τηρηθούν οι αξιώσεις προστασίας του ιδιωτικού βίου και των δεδομένων. Οι προδιαγραφές θα πρέπει να είναι δημόσιες και διαφανείς, όπου είναι δυνατόν, και δεν πρέπει να δημιουργούν αδυναμίες στην υποδομή των επικοινωνιών.

Στο πλαίσιο της σύμβασης της Ευρωπαϊκής Ένωσης για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων,[41] συμφωνήθηκε να διευκολυνθεί η συνεργασία στον τομέα της νόμιμης παρακολούθησης[42]. Η σύμβαση περιλαμβάνει διατάξεις για την παρακολούθηση των τηλεπικοινωνιών μέσω δορυφόρου,[43] και για την παρακολούθηση των επικοινωνιών που πραγματοποιούνται από άτομο που ευρίσκεται στην επικράτεια κάποιου άλλου μέλους.[44] Η Επιτροπή πιστεύει ότι οι κανόνες για την παρακολούθηση των συνδιαλέξεων στη σύμβαση για την αμοιβαία δικαστική συνδρομή αποτελούν προς το παρόν τη μόνη δυνατή λύση. Το κείμενο της σύμβασης είναι ουδέτερο από τεχνολογική άποψη· θα πρέπει να εξεταστεί πως θα λειτουργήσει στην πράξη πριν να μπορέσει να προβλεφθεί οποιαδήποτε βελτίωση. Η Επιτροπή θα εξετάσει τα αποτελέσματα της εφαρμογής της με τα κράτη μέλη, τις επιχειρήσεις, τους χρήστες και τις αρχές ελέγχου της προστασίας δεδομένων κατά τρόπο ώστε να κατοχυρωθεί η αποτελεσματικότητα, η διαφάνεια και η ισορροπημένη κατανομή των πρωτοβουλιών που αναλαμβάνονται στο συγκεκριμένο τομέα.

---

41 ΕΕ C 197 της 12.7.2000, σ. 1. Η σύμβαση θεσπίστηκε στις 29 Μαΐου 2000. Οι διατάξεις της σύμβασης για την παρακολούθηση ισχύουν μόνο στα κράτη μέλη της Ευρωπαϊκής Ένωσης και όχι σε τρίτες χώρες.

42 Η σύμβαση προβλέπει ελάχιστες εγγυήσεις όσον αφορά την προστασία του ιδιωτικού βίου και των προσωπικών δεδομένων.

43 Αρχικός στόχος των διαπραγματεύσεων ήταν να δοθούν δυνατότητες παρακολούθησης των συνδιαλέξεων που πραγματοποιούνται από άτομα που χρησιμοποιούν τηλέφωνο μέσω δορυφόρου και ευρίσκονται στην επικράτεια του παρακολουθούντος κράτους μέλους. Από τεχνική άποψη, το νευραλγικό σημείο παρακολούθησης αυτού του είδους επικοινωνιών ευρίσκεται στο επίγειο σταθμό. Ήταν συνεπώς απαραίτητο να αναζητηθεί η τεχνική βοήθεια του κράτους μέλους στην επικράτεια του οποίου ευρίσκεται αυτός ο επίγειος σταθμός. Η σύμβαση προβλέπει δυο δυνατότητες για την επίλυση αυτού του προβλήματος: μια συνοπτική διαδικασία αμοιβαίας δικαστικής συνδρομής, η οποία απαιτεί ατομικές αιτήσεις παροχής βοήθειας προς το κράτος μέλος που κατέχει αυτόν τον επίγειο σταθμό, και μια τεχνική λύση που στηρίζεται στην εξ αποστάσεως πρόσβαση στον επίγειο σταθμό που πραγματοποιείται από το παρακολουθούν κράτος μέλος, η οποία δεν απαιτεί καμία αίτηση.

44 Η σύμβαση αποτελεί επίσης νομικό πλαίσιο για τις αιτήσεις παρακολούθησης συνδιαλέξεων που πραγματοποιούνται από άτομο που ευρίσκεται στην επικράτεια κάποιου άλλου κράτους μέλους (κράτος μέλος προς το οποίο απευθύνεται η αίτηση). Στη συγκεκριμένη περίπτωση, το παρακολουθούν κράτος μέλος και το κράτος μέλος προς το οποίο απευθύνεται η αίτηση πρέπει αμφότερα να διαθέτουν εντολή παρακολούθησης δυνάμει του αντίστοιχου εθνικού τους δικαίου. Τέλος, η σύμβαση ορίζει τους κανόνες που ισχύουν σε περιπτώσεις κατά τις οποίες το παρακολουθούν κράτος μέλος μπορεί να έχει τη δυνατότητα να παρακολουθήσει επικοινωνίες ατόμου που ευρίσκεται στην επικράτεια κάποιου άλλου κράτους μέλους χωρίς να οφείλει να ζητήσει τη τεχνική βοήθεια αυτού του κράτους μέλους.

Η καταχρηστική και άνευ διακρίσεως εκμετάλλευση των δυνατοτήτων παρακολούθησης, ιδιαίτερα διεθνώς, θα δημιουργήσει προβλήματα σε σχέση με τα δικαιώματα του ατόμου και θα υποσκάψει την εμπιστοσύνη των πολιτών στην κοινωνία της πληροφορίας. Η Επιτροπή αντιμετωπίζει με ανησυχία ορισμένες εκθέσεις για εικαζόμενες καταχρήσεις των δυνατοτήτων παρακολούθησης.[45]

5.2. Διατήρηση δεδομένων κίνησης

Για την έρευνα και δίωξη εγκλημάτων που συνεπάγονται τη χρήση των δικτύων επικοινωνιών, κυρίως του Διαδικτύου, οι υπηρεσίες δίωξης χρησιμοποιούν συχνά δεδομένα κίνησης όταν αυτά αποθηκεύονται από τον φορέα παροχής υπηρεσιών, για σκοπούς χρέωσης. Στο βαθμό που η τιμή που επιβάλλεται για επικοινωνία εξαρτάται ολοένα και λιγότερο από την απόσταση και τον προορισμό και οι φορείς παροχής υπηρεσιών εξελίσσονται προς την κατεύθυνση κατ΄ αποκοπής χρέωσης, η ανάγκη αποθήκευσης των δεδομένων κίνησης για σκοπούς χρέωσης τείνει να εξαφανιστεί. Οι υπηρεσίες δίωξης φοβούνται ότι κατά αυτόν τον τρόπο θα μειωθούν τα υλικά στοιχεία που χρειάζονται για τις ποινικές έρευνες και ζητούν κατά συνέπεια από τους φορείς παροχής υπηρεσιών να διατηρούν αυτά τα δεδομένα για μια ελάχιστη περίοδο προκειμένου να μπορούν να τα χρησιμοποιήσουν για σκοπούς εφαρμογής του νόμου.[46]

Σύμφωνα με τις κοινοτικές οδηγίες για την προστασία των δεδομένων προσωπικού χαρακτήρα, και ειδικότερα με τις γενικές αρχές της οδηγίας 95/46/ΕΚ και τις ειδικότερες διατάξεις της οδηγίας 97/66/ΕΚ, τα δεδομένα κίνησης πρέπει να εξαλείφονται ή να καθίστανται ανώνυμα αμέσως μετά το πέρας της επικοινωνίας, εκτός εάν είναι απαραίτητα για σκοπούς χρέωσης. Στην περίπτωση κατ΄ αποκοπήν ή δωρεάν πρόσβασης στις υπηρεσίες τηλεπικοινωνιών, οι φορείς παροχής υπηρεσιών δεν έχουν καταρχήν δικαίωμα να διατηρούν δεδομένα κίνησης.

Σύμφωνα με αυτές τις ίδιες οδηγίες, τα κράτη μέλη δύνανται να λαμβάνουν νομοθετικά μέτρα για να περιορίσουν την εμβέλεια της υποχρέωσης εξάλειψης δεδομένων κίνησης εφόσον αυτό αποτελεί αναγκαίο μέτρο για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών παραβάσεων ή άνευ αδείας χρησιμοποίησης των τηλεπικοινωνιακών συστημάτων.[47]

Εντούτοις, οποιοδήποτε νομοθετικό μέτρο σε εθνικό επίπεδο προβλέπει ενδεχομένως τη διατήρηση δεδομένων κίνησης με στόχο την εφαρμογή του νόμου χρειάζεται να πληροί ορισμένες προϋποθέσεις: το προτεινόμενο μέτρο χρειάζεται να είναι κατάλληλο, απαραίτητο και ανάλογο όπως αξιώνει το κοινοτικό και διεθνές δίκαιο, καθώς επίσης οι οδηγίες 97/66/ΕΚ και 95/46/ΕΚ, η Ευρωπαϊκή Σύμβαση προστασίας των ανθρωπίνων δικαιωμάτων της 4ης Νοεμβρίου 1950 και η σύμβαση του Συμβουλίου της Ευρώπης, της 28ης Ιανουαρίου 1981, για την προστασία των προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού

---

45 Μια εκτεταμένη και λεπτομερής έκθεση του κ. Campbell (http://www.gn.apc.org/duncan/stoa_cover.htm) για ένα σύστημα παρακολούθησης καλούμενο ECHELON αποτέλεσε το θέμα δημόσιας ακρόασης του Ευρωπαϊκού Κοινοβουλίου. Η έκθεση προσδιορίζει ότι το σύστημα ECHELON σχεδιάστηκε για τις ανάγκες της εθνικής ασφάλειας αλλά χρησιμοποιείται επίσης για ενέργειες βιομηχανικής κατασκοπείας. Το Ευρωπαϊκό Κοινοβούλιο δημιούργησε προσωρινή επιτροπή επιφορτισμένη με το καθήκον να μελετήσει το θέμα και να υποβάλλει έκθεση στην ολομέλεια εντός έτους.

46 Αυτό περιλαμβάνει ποινικές έρευνες σε υποθέσεις που δεν έχουν σχέση με ηλεκτρονικούς υπολογιστές ή δίκτυα επικοινωνίας, αλλά στις οποίες τα δεδομένα μπορούν να χρησιμεύσουν για τη διερεύνηση του εγκλήματος.

47 Άρθρο 14 της οδηγίας 97/66/ΕΚ και άρθρο 13 της οδηγίας 95/46/ΕΚ.

χαρακτήρα. Η τήρηση αυτών των αρχών καθίσταται πιο αναγκαία για τα μέτρα που συνεπάγονται τη συστηματική διατήρηση δεδομένων για μεγάλο τμήμα του πληθυσμού.

Ορισμένα κράτη μέλη αναλαμβάνουν νομοθετικές πρωτοβουλίες προκειμένου να υποχρεώσουν ή να εξουσιοδοτήσουν τους φορείς παροχής υπηρεσιών να αποθηκεύουν ορισμένες κατηγορίες δεδομένων κίνησης, μετά την παροχή της υπηρεσίας τα οποία δεν είναι μεν απαραίτητα για σκοπούς χρέωσης, αλλά μπορούν να θεωρηθούν χρήσιμα για ποινικές έρευνες. Η έκταση και η μορφή αυτών των πρωτοβουλιών ποικίλει σημαντικά ανάλογα με το κράτος, αλλά όλες στηρίζονται στην ιδέα ότι θα πρέπει να τίθενται στη διάθεση των υπηρεσιών δίωξης περισσότερα στοιχεία από αυτά που χρειάζονται απλά και μόνο για τις ανάγκες της παροχής υπηρεσίας. Η Επιτροπή εξετάζει αυτά τα μέτρα υπό το φως της ισχύουσας κοινοτικής νομοθεσίας.

Το Ευρωπαϊκό Κοινοβούλιο προσδίδει ιδιαίτερη προσοχή στα προβλήματα προστασίας του ιδιωτικού βίου και γενικά διάκειται ευνοϊκά απέναντι στην ισχυρή προστασία των δεδομένων προσωπικού χαρακτήρα. Εντούτοις, κατά τις συζητήσεις για την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο, διατύπωσε γνώμη η οποία ευνοεί τη γενική υποχρέωση διατήρησης δεδομένων κίνησης για περίοδο τριών μηνών.[48]

Αυτή η θέση καταδεικνύει τη σημασία του πλαισίου εντός του οποίου εγγράφεται η εξέταση ενός τόσο ευαίσθητου θέματος όπως είναι η διατήρηση των δεδομένων κίνησης και την πρόκληση που αντιμετωπίζουν οι αρμόδιοι για τη χάραξη πολιτικής κατά την αναζήτηση ισορροπιών.

Η Επιτροπή θεωρεί ότι οποιαδήποτε λύση στο πολύπλοκο θέμα της διατήρησης δεδομένων κίνησης πρέπει να είναι καλά θεμελιωμένη, ανάλογη προς το στόχο της και να εξασφαλίζει δίκαιη ισορροπία μεταξύ των διακυβευόμενων συμφερόντων. Μόνο μια προσέγγιση η οποία θα συνδύαζε την εμπειρογνωμοσύνη και τις ικανότητες των δημοσίων αρχών, των επιχειρήσεων, των αρχών που είναι αρμόδιες για την προστασία των δεδομένων και των χρηστών θα επιτύγχανε να συμβιβάσει αυτούς τους στόχους. Θα ήταν άκρως ευκταία μια συνεκτική προσέγγιση σε όλα τα κράτη μέλη σχετικά με αυτό το πολύπλοκο θέμα για να επιτευχθούν οι στόχοι της αποτελεσματικότητας και της αναλογικότητας και να αποφευχθεί η δημιουργία κατάστασης στην οποία οι αρχές δίωξης και η κοινότητα του Διαδικτύου θα ευρίσκονταν αντιμέτωποι με ένα συνοθύλευμα διαφόρων τεχνικών και νομικών πλαισίων.

Πρέπει να ληφθούν υπόψη σημαντικά αλλά πολύ διαφορετικά συμφέροντα. Από τη μια πλευρά, οι αρχές ελέγχου που είναι επιφορτισμένες με την προστασία των δεδομένων είναι της άποψης ότι το πλέον αποτελεσματικό μέσο για τη μείωση απαράδεκτων κινδύνων για τον ιδιωτικό βίο αναγνωρίζοντας ταυτόχρονα την ανάγκη αποτελεσματικής εφαρμογής του νόμου είναι να μη διατηρούνται κατ΄αρχήν τα δεδομένα κίνησης αποκλειστικά και μόνο για σκοπούς εφαρμογής του νόμου.[49] Από την άλλη πλευρά, οι αρχές εφαρμογής του νόμου

---

48 Νομοθετικό ψήφισμα που αποτελεί τη γνώμη του Ευρωπαϊκού Κοινοβουλίου για το σχέδιο κοινής δράσης, που εγκρίθηκε από το Συμβούλιο στη βάση του άρθρου K.3 της Συνθήκης για την Ευρωπαϊκή Ένωση, για την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο, Τροπολογία 17 (ΕΕ C 219,30.7.1999, σ. 68 και κυρίως σ. 71).

49 "Μεγάλης κλίμακας διερευνητική ή γενική παρακολούθηση πρέπει να απαγορεύεται…το πιο αποτελεσματικό μέσο για τη μείωση απαράδεκτων κινδύνων για τον ιδιωτικό βίο ενώ ταυτόχρονα θα αναγνωρίζονται οι ανάγκες για αποτελεσματική εφαρμογή του νόμου είναι τα δεδομένα κίνησης καταρχήν να μη διατηρούνται αποκλειστικά και μόνο για σκοπούς εφαρμογής του νόμου και οι εθνικές νομοθεσίες να μην υποχρεώνουν τους φορείς τηλεπικοινωνιών, τις υπηρεσίες τηλεπικοινωνιών και τους φορείς παροχής υπηρεσιών Διαδικτύου να διατηρούν δεδομένα κίνησης για περίοδο μεγαλύτερη από ό,τι χρειάζεται για σκοπούς χρέωσης", Σύσταση 3/99 της 7ης Σεπτεμβρίου 1999, της ομάδας εργασίας

έχουν δηλώσει ότι θεωρούν ότι η διατήρηση ενός ελάχιστου όγκου δεδομένων κίνησης για μια ελάχιστη περίοδο θα ήταν απαραίτητη για τη διευκόλυνση των ποινικών ερευνών.

Οι επιχειρήσεις έχουν συμφέρον να συνεργαστούν για την καταπολέμηση της εγκληματικότητας που λαμβάνει τη μορφή ηλεκτρονικής πειρατείας ή απάτης, χωρίς όμως να προσκρούουν σε μέτρα αδικαιολόγητα υψηλού κόστους. Οι οικονομικές επιπτώσεις των μέτρων που θα ληφθούν στο συγκεκριμένο θέμα πρέπει να αναλυθούν προσεκτικά και να συγκριθούν με την αποτελεσματικότητα των εν λόγω μέτρων όσον αφορά την καταπολέμηση του εγκλήματος πληροφορικής προκειμένου να αποφευχθεί το ενδεχόμενο να καταστεί το Διαδίκτυο πιο δαπανηρό και οικονομικά ασύμφορο για τους χρήστες. Θα πρέπει να εξασφαλιστεί επαρκής ασφάλεια για όλα τα διατηρούμενα δεδομένα κίνησης.

Σε κάθε περίπτωση οι επιχειρήσεις θα διαδραματίσουν ρόλο κλειδί συμβάλλοντας στη διαδικασία δημιουργίας μιας πιο ασφαλούς κοινωνίας της πληροφορίας. Θα πρέπει οι χρήστες να έχουν εμπιστοσύνη στην ασφάλεια της κοινωνίας της πληροφορίας και να αισθάνονται προστατευμένοι από παραβάσεις και προσβολές του ιδιωτικού τους βίου.

Η Επιτροπή υποστηρίζει και ενθαρρύνει ανεπιφύλακτα την εγκαθίδρυση εποικοδομητικού διαλόγου μεταξύ των αρχών εφαρμογής του νόμου, των επιχειρήσεων, των αρχών που είναι επιφορτισμένες με την προστασία των δεδομένων, των οργανώσεων των καταναλωτών και των άλλων δυνάμει ενδιαφερομένων. Στο πλαίσιο του προβλεπόμενου φόρουμ της Ευρωπαϊκής Ένωσης (βλέπε σημείο 6.4 της παρούσας ανακοίνωσης), η Επιτροπή θα καλέσει όλους τους ενδιαφερόμενους να προβούν, κατά προτεραιότητα, σε εμπεριστατωμένη εξέταση του πολύπλοκου ζητήματος της διατήρησης των δεδομένων κίνησης με σκοπό να εξευρεθούν από κοινού οι κατάλληλες, ισορροπημένες και αναλογικές λύσεις τηρουμένων των θεμελιωδών δικαιωμάτων προστασίας του ιδιωτικού βίου και των δεδομένων[50]. Στη βάση των αποτελεσμάτων αυτής της εξέτασης, η Επιτροπή θα είναι σε θέση να αξιολογήσει την ανάγκη θέσπισης νομοθετικών ή άλλων μέτρων στο επίπεδο της Ευρωπαϊκής Ένωσης.

5.3. Ανώνυμη πρόσβαση και χρήση

Οι εμπειρογνώμονες στα θέματα εφαρμογής του νόμου έχουν εκφράσει ανησυχίες για το γεγονός ότι η ανωνυμία μπορεί να καταλήξει σε απουσία ευθύνης και να παρεμποδίσει σοβαρά τη δυνατότητα σύλληψης ορισμένων εγκληματιών. Η ανώνυμη χρήση του κινητού τηλεφώνου είναι εφικτή σε ορισμένες χώρες (ενώ σε άλλες όχι) χάρη στις προπληρωμένες κάρτες. Η ανώνυμη πρόσβαση και χρήση του Διαδικτύου προτείνεται από ορισμένους φορείς παροχής υπηρεσιών ή πρόσβασης, συμπεριλαμβανομένων των ανώνυμων επαναποστολέων και των καφενείων στο Διαδίκτυο. Ένας βαθμός ανωνυμίας διευκολύνεται επίσης από το σύστημα δυναμικής διευθυνσιοδότησης στο Διαδίκτυο στο οποίο οι διευθύνσεις δε χορηγούνται στους χρήστες σε μόνιμη βάση αλλά μόνο κατά τη διάρκεια ορισμένης περιόδου.

Στις συζητήσεις τους με την Επιτροπή, ορισμένοι αντιπρόσωποι των επιχειρήσεων φάνηκαν εχθρικά διακείμενοι στην πλήρη ανωνυμία, εν μέρει για λόγους που συνδέονται με τη δική τους ασφάλεια, την καταπολέμηση της απάτης και την ακεραιότητα των δικτύων. Το London Internet Exchange επέστησε την προσοχή στις κατευθυντήριες γραμμές σχετικά με τις

για την προστασία δεδομένων του άρθρου 29, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[50] Όπως ενσωματώνεται στην Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων (άρθρο 8, δικαίωμα προστασίας του ιδιωτικού βίου), τον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, τη Συνθήκη ΕΕ και τις οδηγίες ΕΚ για την προστασία δεδομένων.

βέλτιστες πρακτικές τις οποίες έχει δημοσιεύσει και οι οποίες έχουν αποδειχθεί ιδιαιτέρως χρήσιμες στο Ηνωμένο Βασίλειο.[51] Εντούτοις, άλλοι αντιπρόσωποι επιχειρήσεων και ειδικοί στα θέματα προστασίας του ιδιωτικού βίου δήλωσαν ότι χωρίς ανωνυμία είναι αδύνατον να κατοχυρώσουν τα θεμελιώδη δικαιώματα.

Η ομάδα εργασίας για την προστασία δεδομένων που έχει συσταθεί δυνάμει του άρθρου 29 έχει εκδώσει σύσταση για το θέμα της ανώνυμης χρήσης του Διαδικτύου.[52] Θεωρεί ότι το θέμα της ανωνυμίας στο Διαδίκτυο ευρίσκεται στο κέντρο διλήμματος το οποίο πρέπει να αντιμετωπίσουν οι κυβερνήσεις και οι διεθνείς οργανώσεις. Από τη μια πλευρά, η δυνατότητα διατήρησης της ανωνυμίας είναι ουσιαστική εφόσον επιδιώκεται η προάσπιση των θεμελιωδών δικαιωμάτων που αφορούν τον ιδιωτικό βίο και την ελευθερία έκφρασης στον κυβερνοχώρο. Από την άλλη πλευρά, η δυνατότητα συμμετοχής σε δραστηριότητες ηλεκτρονικής επικοινωνίας χωρίς να αποκαλύπτεται η ταυτότητα αντιβαίνει σε πρωτοβουλίες που αναλαμβάνονται για να υποστηριχθούν άλλες δραστηριότητες γενικού συμφέροντος όπως η καταπολέμηση του παράνομου και επιζήμιου περιεχομένου, η καταπολέμηση των οικονομικών εγκλημάτων ή των παραβάσεων των δικαιωμάτων πνευματικής ιδιοκτησίας. Αυτή η εμφανής σύγκρουση διαφόρων στόχων γενικού συμφέροντος δεν είναι βέβαια καινοφανής. Στο πλαίσιο των πιο παραδοσιακών τρόπων επικοινωνίας off-line όπως είναι οι ταχυδρομικές υπηρεσίες και οι υπηρεσίες αποστολής δεμάτων, το τηλέφωνο, οι εφημερίδες ή οι υπηρεσίες ραδιοφωνίας και τηλεόρασης, έχει επιτευχθεί ισορροπία μεταξύ αυτών των στόχων. Η πρόκληση την οποία πρέπει να αντιμετωπίζουν σήμερα οι πολιτικά αρμόδιοι είναι να εξασφαλιστεί αυτή η ισορροπημένη προσέγγιση, η οποία κατοχυρώνει βασικά δικαιώματα ενώ ταυτόχρονα επιτρέπει ανάλογους περιορισμούς αυτών των δικαιωμάτων σε περιορισμένες και ειδικές περιστάσεις, στο νέο πλαίσιο του κυβερνοχώρου. Η έκταση και τα όρια της ανωνυμίας των ατόμων που εκφράζονται on-line θα είναι καθοριστικής σημασίας για αυτή την ισορροπία.

Στην τελική διακήρυξη της υπουργικής διάσκεψης για τα παγκόσμια ηλεκτρονικά δίκτυα η οποία έλαβε χώρα στη Βόννη από τις 6-8 Ιουλίου 1997, η αρχή που υποστηρίχθηκε ήταν ότι ο χρήστης πρέπει να μπορεί να επιλέξει να παραμείνει ανώνυμος on-line εφόσον έχει την ίδια επιλογή off-line. Υπάρχει ως εκ τούτου σαφής συμφωνία για το γεγονός ότι οι δραστηριότητες που ασκούνται στα δίκτυα πρέπει να εξεταστούν εφαρμόζοντας τις ίδιες βασικές νομικές αρχές που ισχύουν οπουδήποτε αλλού. Το Διαδίκτυο δεν είναι ένα αναρχικό γκέτο στο οποίο δεν ισχύουν οι κανόνες της κοινωνίας. Επίσης, η ικανότητα των κυβερνήσεων και των δημόσιων αρχών να περιορίσουν τα δικαιώματα των ατόμων και να ελέγξουν δυνάμει παράνομες συμπεριφορές δεν πρέπει να είναι μεγαλύτερη στα δημόσια δίκτυα από ό,τι συμβαίνει σε άλλους τομείς off-line. Η αξίωση σύμφωνα με την οποία οι περιορισμοί των θεμελιωδών δικαιωμάτων και ελευθεριών πρέπει να είναι δεόντως δικαιολογημένοι απαραίτητοι και ανάλογοι ενόψει άλλων στόχων δημόσιας πολιτικής πρέπει να ισχύει επίσης στον κυβερνοχώρο.

Στη σύσταση της ομάδας εργασίας του άρθρου 29 για την προστασία δεδομένων ορίζεται λεπτομερώς ο τρόπος με τον οποίο αυτό μπορεί να επιτευχθεί σε ειδικές περιπτώσεις (για παράδειγμα όσον αφορά το ηλεκτρονικό ταχυδρομείο, τα φόρουμ συζητήσεων, κλπ).[53] Η Επιτροπή συντάσσεται με τις θέσεις που εκφράστηκαν από την ομάδα εργασίας.

---

51 http://www.linx.net/noncore/bcp/.

52 Ομάδα εργασίας για την προστασία των ατόμων έναντι της επεξεργασίας προσωπικών δεδομένων. Σύσταση 3/97 Ανωνυμία στο Διαδίκτυο, εγκρίθηκε από την ομάδα εργασίας στις 3 Δεκεμβρίου 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm .

5.4. Πρακτική συνεργασία σε διεθνές επίπεδο

Πρόσφατα ενέργειες καταστολής που διεξήχθησαν από κοινού σε παγκόσμιο επίπεδο, όπως οι ενέργειες Starburst και Cathedral κατά των δικτύων παιδοφιλίας, απέδειξαν ότι είναι χρήσιμο για τις υπηρεσίες δίωξης και τις δικαστικές αρχές να συντονίζουν τη δράση τους σε διεθνές επίπεδο, τόσο με την ανταλλαγή πληροφοριών σε προκαταρκτικό στάδιο όσο και εμποδίζοντας τα άλλα μέλη του δικτύου να γνωρίζουν τη στιγμή κατά την οποία θα πραγματοποιηθούν συλλήψεις και κατασχέσεις. Το Διαδίκτυο απεδείχθη πολύτιμο και αποτελεσματικό εργαλείο για αστυνομικές και τελωνειακές έρευνες όταν χρησιμοποιείται ως μέσο για τη διάπραξη παραδοσιακών εγκλημάτων, όπως η παραποίηση και το λαθρεμπόριο. Από την άλλη πλευρά, αυτές οι ενέργειες έφεραν στο φως σοβαρές νομικές και λειτουργικές δυσκολίες στις οποίες προσέκρουσαν οι υπηρεσίες δίωξης και οι δικαστικές αρχές κατά τη διεξαγωγή αυτής της δράσης, όπως η προετοιμασία διασυνοριακής αποδεικτικής διαδικασίας ή αίτησης για τη διενέργεια διαδικαστικών πράξεων, η αναγνώριση θυμάτων, και ο ρόλος των διακυβερνητικών οργανώσεων που ασχολούνται με αστυνομικά θέματα (Interpol και Europol).

Στον τομέα των συγκεκριμένων μέτρων διεθνούς συνεργασίας, τα διεθνή δίκτυα ανταλλαγής πληροφοριών αποκτούν αυξανόμενη σημασία για τις αστυνομικές και τελωνειακές αρχές.

Στο πλαίσιο των χωρών του G8 έχει ήδη δημιουργηθεί και είναι ήδη λειτουργικό ένα δίκτυο πληροφόρησης το οποίο λειτουργεί 24 ώρες το 24ωρο, και τις επτά ημέρες της εβδομάδας, το οποίο συγκεντρώνει τα σημεία επαφής των αρμοδίων για την εφαρμογή του νόμου αρχών. Κύριος σκοπός του είναι να δέχεται και να απαντά σε επείγουσες αιτήσεις συνεργασίας σε περιπτώσεις στις οποίες απαιτούνται ηλεκτρονικές αποδείξεις. Αυτό το δίκτυο έχει χρησιμοποιηθεί με επιτυχία σε ορισμένες υποθέσεις. Το Συμβούλιο ΔΕΥ της 19ης Μαρτίου 1998 ενέκρινε τις 10 αρχές καταπολέμησης του εγκλήματος υψηλής τεχνολογίας, που θεσπίστηκαν από τις χώρες του G8 και κάλεσε τα κράτη μέλη της Ευρωπαϊκής Ένωσης που δεν αποτελούν μέλη της ομάδας G8 να προσχωρήσουν στο δίκτυο[54]. Αυτά τα σημεία επαφής πρέπει να συνεργάζονται απευθείας, συμπληρώνοντας τις υπάρχουσες δομές αμοιβαίας βοήθειας και τα κανάλια επικοινωνίας.[55]

Η δημιουργία ενός τέτοιου δικτύου προβλέπεται επίσης από το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης. Η μνεία ενός δικτύου σημείων επαφής που λειτουργούν 24 ώρες το 24ωρο, και τις 7 ημέρες της εβδομάδας, αναφέρεται επίσης στην απόφαση του Συμβουλίου σχετικά με την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο και στην κοινή θέση της Ευρωπαϊκής Ένωσης σχετικά με το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο[56] και στην απόφαση του Συμβουλίου η οποία εγκρίνει το

---

54 Πέρα από τα μέλη G8, πέντε κράτη μέλη της ΕΕ έχουν προσχωρήσει μέχρι τώρα στο δίκτυο G8 24/7.

55 Κατά το παγκόσμιο συνέδριο κατά της σεξουαλικής εκμετάλλευσης των παιδιών για εμπορικούς σκοπούς, το οποίο πραγματοποιήθηκε στη Στοκχόλμη στις 28 Αυγούστου 1996, υποβλήθηκαν προτάσεις με σκοπό να ενσωματωθεί η INTERPOL στα προαναφερόμενα δίκτυα. Η απόφαση του Συμβουλίου της Ευρωπαϊκής Ένωσης σχετικά με την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο προβλέπει επίσης την παρέμβαση της Europol στο συγκεκριμένο τομέα.

56 Άρθρο 1.4 της κοινής θέσης: "Τα κράτη μέλη θα πρέπει να στηρίζουν τη θέσπιση διατάξεων που θα διευκολύνουν τη διεθνή συνεργασία περιλαμβάνοντας, στο μεγαλύτερο δυνατό βαθμό, διατάξεις σχετικά με την αμοιβαία δικαστική συνδρομή. Η σύμβαση θα πρέπει να διευκολύνει την ταχεία συνεργασία για την καταπολέμηση των εγκλημάτων πληροφορικής και των εγκλημάτων που διαπράττονται με τη βοήθεια ηλεκτρονικών υπολογιστών. Αυτή η μορφή συνεργασίας μπορεί να περιλαμβάνει τη δημιουργία σημείων επαφής των αρχών εφαρμογής του νόμου που θα λειτουργούν σε 24ωρη βάση, τα οποία θα συμπληρώνουν τις υφιστάμενες δομές αμοιβαίας συνδρομής."

σχέδιο δράσης της ομάδας των G8[57], αλλά η Ευρωπαϊκή Ένωση δεν έχει προς το παρόν λάβει συγκεκριμένα μέτρα σχετικά με το θέμα αυτό.

Η Επιτροπή θεωρεί ότι, δεδομένης της ανάγκης που υπάρχει στο συγκεκριμένο τομέα για δέουσα εμπειρογνωμοσύνη και ταχεία δράση, επείγει να τεθούν σε εφαρμογή οι προθέσεις του Συμβουλίου. Προκειμένου να μπορεί να λειτουργεί με ικανοποιητικό τρόπο, αυτό το δίκτυο θα πρέπει εντούτοις να διαθέτει αρμόδιο προσωπικό τόσο σε νομικό όσο και σε τεχνικό επίπεδο, γεγονός που προϋποθέτει την αντίστοιχη κατάρτιση.

Είναι εξίσου απαραίτητο να εντατικοποιηθεί η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των τελωνειακών αρχών. Οι υφιστάμενες μορφές συνεργασίας θα πρέπει να βελτιωθούν και πρέπει να αναπτυχθούν νέα μέσα για τη διεξαγωγή κοινών ενεργειών και την ανταλλαγή πληροφοριών. Δεδομένων των αξιώσεων προστασίας των δεδομένων, οι τελωνειακές αρχές συμφωνούν ολοένα και περισσότερο στην ανάγκη να δημιουργηθούν διεθνή δίκτυα πληροφόρησης για να διευκολυνθούν περαιτέρω οι ανταλλαγές πληροφοριών. Πρέπει επίσης να επενδυθούν περισσότεροι πόροι στο συγκεκριμένο τομέα, τόσο για τον εκσυγχρονισμό των συστημάτων πληροφορικής όσο και για την κατάρτιση του προσωπικού, προκειμένου να δοθεί στις τελωνειακές αρχές η δυνατότητα να εκτελούν με μεγαλύτερη αποτελεσματικότητα τα καθήκοντά τους.

5.5. Εξουσίες και δικαιοδοσία στον τομέα του δικονομικού δικαίου

Σε εθνικό επίπεδο, εφόσον πληρωθούν οι απαραίτητες νομοθετικές προϋποθέσεις, οι αρχές εφαρμογής του νόμου πρέπει να είναι σε θέση να αναζητούν και να κατάσχουν δεδομένα αποθηκευμένα σε ηλεκτρονικούς υπολογιστές αρκετά γρήγορα ώστε να εμποδίζουν την καταστροφή αποδεικτικών στοιχείων. Οι αρχές εφαρμογής του νόμου θεωρούν ότι πρέπει να διαθέτουν επαρκείς εξουσίες εξαναγκασμού ώστε να μπορούν, στο πλαίσιο των αρμοδιοτήτων τους, να προβαίνουν σε έρευνα των ηλεκτρονικών συστημάτων και σε κατάσχεση δεδομένων, να διατάσσουν άτομα να υποβάλλουν συγκεκριμένα ηλεκτρονικά δεδομένα, να διατάσσουν ή να επιτυγχάνουν την ταχεία διατήρηση συγκεκριμένων δεδομένων σύμφωνα με τις κανονικές νομικές εγγυήσεις και διαδικασίες. Προς το παρόν, εντούτοις δεν έχει γίνει προσέγγιση των εγγυήσεων και των διαδικασιών.

Μπορούν να ανακύψουν προβλήματα όταν, κατά την πρόσβαση σε ηλεκτρονικό υπολογιστή, οι αρχές εφαρμογής του νόμου διαπιστώνουν ότι ορισμένοι εκ των ηλεκτρονικών υπολογιστών και των δικτύων που συμμετέχουν ευρίσκονται σε όλη τη χώρα. Αυτά τα θέματα καθίστανται ακόμα πιο πολύπλοκα όταν, κατά τη στιγμή της έρευνας σε ηλεκτρονικό υπολογιστή ή απλής έρευνας, κάποιο όργανο εφαρμογής του νόμου διαπιστώνει ότι συμβουλεύεται δεδομένα που ευρίσκονται σε μια ή περισσότερες χώρες. Διακυβεύονται και πρέπει να εξισορροπηθούν σημαντικά συμφέροντα εθνικής κυριαρχίας, ανθρωπίνων δικαιωμάτων και εφαρμογής του νόμου.

Τα υφιστάμενα νομικά μέσα στον τομέα της διεθνούς συνεργασίας σε ποινικές υποθέσεις (αμοιβαία δικαστική συνδρομή) μπορούν να αποδειχθούν ακατάλληλα ή ανεπαρκή, επειδή η εφαρμογή τους χρειάζεται κανονικά μερικές ημέρες, εβδομάδες ή μήνες. Πρέπει να δημιουργηθεί ένας μηχανισμός με τον οποίο, στην περίπτωση των διασυνοριακών ποινικών διαδικασιών, οι χώρες θα μπορούν, με ταχύτητα και αποτελεσματικότητα, να πραγματοποιούν έρευνες για τις παραβάσεις και να συγκεντρώνουν αποδεικτικά στοιχεία ή, τουλάχιστον, να μην χάνουν σημαντικά αποδεικτικά στοιχεία, κατά τρόπο που να

---

[57] Διατίθεται στη διεύθυνση του Ευρωπαϊκού Δικαστικού δικτύου http://ue.eu.int/ejn/index.htm.

συμβιβάζεται με τις αρχές της εθνικής κυριαρχίας, τα συνταγματικά δικαιώματα και τα δικαιώματα του ατόμου, συμπεριλαμβανομένης της προστασίας του ιδιωτικού βίου και των δεδομένων.

Οι νέες προτάσεις που προβλέπονται από το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο προκειμένου να αντιμετωπιστούν αυτά τα προβλήματα περιλαμβάνουν δικαστικές εντολές για τη διατήρηση δεδομένων προκειμένου να διευκολυνθούν ειδικές έρευνες. Εντούτοις, άλλα θέματα, όπως οι διασυνοριακές έρευνες και κατασχέσεις, θέτουν δύσκολα ζητήματα ουσίας τα οποία δεν έχουν μέχρι τώρα επιλυθεί. Όλοι οι ενδιαφερόμενοι θα πρέπει να προβούν σε πιο εμπεριστατωμένη εξέταση του θέματος πριν να καταστεί δυνατή η ανάληψη συγκεκριμένων πρωτοβουλιών.

Η υποομάδα του G8 που είναι επιφορτισμένη με το έγκλημα υψηλής τεχνολογίας συζήτησε το θέμα της διασυνοριακής έρευνας και κατάσχεσης και επέτυχε συμφωνία σε προσωρινές αρχές, εν αναμονή της μεταγενέστερης σύναψης συμφωνίας μονιμότερου χαρακτήρα[58]. Τίθενται εντούτοις σημαντικά ζητήματα, κυρίως όσον αφορά τις προϋποθέσεις υπό τις οποίες είναι δυνατόν να πραγματοποιηθούν έρευνες και κατασχέσεις στο πλαίσιο συνοπτικής διαδικασίας πριν να ενημερωθεί σχετικά το κράτος στο εσωτερικό του οποίου αυτές πραγματοποιούνται, προκειμένου να εξασφαλιστεί η τήρηση των θεμελιωδών δικαιωμάτων. Στην κοινή τους θέση όσον αφορά το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, οι Υπουργοί του Συμβουλίου της Ευρωπαϊκής Ένωσης υιοθέτησαν ανοικτή θέση.[59]

Στις υποθέσεις διασυνοριακών εγκλημάτων πληροφορικής είναι επίσης σημαντικό να υπάρχουν σαφείς κανόνες που να καθορίζουν το κράτος που έχει δικαιοδοσία για την άσκηση διώξεων. Θα πρέπει κυρίως να αποφευχθεί το ενδεχόμενο να μην υπάρχει δικαιοδοσία κανενός κράτους. Το σχέδιο σύμβασης του Συμβουλίου της Ευρώπης προτείνει κυρίως να αναγνωρίζεται η δικαιοδοσία κάποιου κράτους όταν το ποινικό αδίκημα διαπράττεται στην επικράτειά του ή από κάποιον υπήκοό του. Όταν υπάρχει δικαιοδοσία περισσοτέρων κρατών, τα εν λόγω κράτη θα πρέπει να διαβουλεύονται μεταξύ τους προκειμένου να αποφασισθεί η πλέον ενδεδειγμένη δικαιοδοσία. Αυτές οι αρχές είναι ορθές αλλά η εφαρμογή τους θα εξαρτηθεί κατά πολύ από την αποτελεσματικότητα των διμερών ή πολυμερών διαβουλεύσεων. Η Επιτροπή θα συνεχίσει την εξέταση αυτού του ζητήματος προκειμένου να καθορίσει το κατά πόσον επιβάλλεται η λήψη συμπληρωματικών μέτρων στο επίπεδο της Ευρωπαϊκής Ένωσης.

Η Επιτροπή, η οποία έλαβε μέρος στις συζητήσεις του Συμβουλίου της Ευρώπης όπως και σε αυτές των χωρών του G8, αναγνωρίζει την πολυπλοκότητα αυτών των θεμάτων και τις δυσκολίες που αντιμετωπίζονται με τα θέματα δικονομικού δικαίου. Είναι εντούτοις ζωτικής σημασίας στο εσωτερικό της Ευρωπαϊκής Ένωσης να διεξάγεται ο αγώνας κατά του

---

58 Ανακοινωθέν της Υπουργικής Διάσκεψης των χωρών του G8 για την καταπολέμηση του διεθνικού οργανωμένου εγκλήματος - Μόσχα, 19-20 Οκτωβρίου 1999 (βλέπε http://www.usdoj.gov/criminal/cybercrime/action.htm και επίσης http://www.usdoj.gov/criminal/cybercrime/principles.htm).

59 ΕΕ L 142/2, 5.6.1999: "Με την επιφύλαξη συνταγματικών αρχών και ειδικών διασφαλίσεων που θα αποσκοπούν στο δέοντα σεβασμό της εθνικής κυριαρχίας, ασφάλειας, δημόσιας τάξης ή άλλων ουσιωδών συμφερόντων άλλων κρατών, είναι δυνατόν να εξετάζεται σε εξαιρετικές περιπτώσεις η διενέργεια διασυνοριακής ηλεκτρονικής έρευνας με σκοπό τη διερεύνηση σοβαρού εγκλήματος, όπως θα καθοριστεί περαιτέρω στη σύμβαση, και ιδίως σε περίπτωση κατεπείγοντος, π.χ. εάν αυτή είναι αναγκαία προκειμένου να αποφευχθεί η καταστροφή ή η τροποποίηση αποδεικτικών στοιχείων για σοβαρή εγκληματική ενέργεια ή να παρεμποδιστεί η διάπραξη εγκληματικής ενέργειας που είναι δυνατόν να οδηγήσει στο θάνατο ή σε σοβαρό τραυματισμό ανθρώπου".

εγκλήματος στον κυβερνοχώρο στο πλαίσιο αποτελεσματικής συνεργασίας, εφόσον επιθυμούμε να καταστήσουμε την κοινωνία των πληροφοριών ασφαλέστερη και να δημιουργηθεί ένας χώρος ελευθερίας, ασφάλειας και δικαιοσύνης.

Η Επιτροπή θα εξακολουθήσει τις διαβουλεύσεις της με όλους τους ενδιαφερόμενους κατά τη διάρκεια των επόμενων μηνών, προκειμένου να εκμεταλλευτεί αυτές τις εργασίες. Αυτό το ζήτημα θα εξεταστεί επίσης στο ευρύτερο πλαίσιο των εργασιών της που αποσκοπούν στην εφαρμογή των συμπερασμάτων του Ευρωπαϊκού Συμβουλίου του Τάμπερε του Οκτωβρίου 1999. Η Διάσκεψη Κορυφής του Τάμπερε ζήτησε συγκεκριμένα από το Συμβούλιο και την Επιτροπή να θεσπίσουν, μέχρι το Δεκέμβριο 2000, ένα πρόγραμμα μέτρων για την εφαρμογή της αρχής της αμοιβαίας αναγνώρισης των δικαστικών αποφάσεων. Η Επιτροπή έχει ήδη δημοσιεύσει ανακοίνωση για την αμοιβαία αναγνώριση των οριστικών αποφάσεων σε ποινικές υποθέσεις[60]. Στο πλαίσιο της συμβολής της στην εφαρμογή του τμήματος του προγράμματος μέτρων που αφορά την εκτέλεση των αποφάσεων που προηγούνται της εκδίκασης, η Επιτροπή πρόκειται να εξετάσει τις δυνατότητες αμοιβαίας αναγνώρισης αυτών των προδικαστικών αποφάσεων που έχουν σχέση με έρευνες στον τομέα του εγκλήματος πληροφορικής, με σκοπό να υποβάλει νομοθετική πρόταση δυνάμει του τίτλου VI της Συνθήκης για την Ευρωπαϊκή Ένωση.

5.6. Αποδεικτική αξία των ηλεκτρονικών δεδομένων

Ακόμα και όταν έχουν πρόσβαση σε ηλεκτρονικά δεδομένα που φαίνεται να αποτελούν αποδεικτικά στοιχεία ποινικής παράβασης, οι αρχές εφαρμογής του νόμου πρέπει να είναι σε θέση να τα επεξεργαστούν και να τα επικυρώσουν, προκειμένου να μπορούν να τα χρησιμοποιήσουν για τις ποινικές έρευνες και διώξεις. Αυτό δεν αποτελεί εύκολο καθήκον δεδομένου του ασταθούς και πρόσφορου σε μεταβολή, πλαστογράφηση, τεχνική προστασία ή διαγραφή χαρακτήρα των ηλεκτρονικών δεδομένων. Αυτή η εργασία ανατίθεται στις υπηρεσίες ηλεκτρονικής εγκληματολογίας, που είναι επιφορτισμένες με την ανάπτυξη και τη χρήση επιστημονικών πρωτοκόλλων και διαδικασιών για την αναζήτηση ηλεκτρονικών αποδεικτικών στοιχείων, την ανάλυση και την διατήρηση της γνησιότητας των δεδομένων που συνελέγησαν.

Η Διεθνής Οργάνωση Ηλεκτρονικών Αποδείξεων (IOCE) δέχθηκε, κατόπιν αιτήσεως των εμπειρογνωμόνων της ομάδας G8, να επεξεργαστεί συστάσεις για πρότυπα, συμπεριλαμβανομένου του καθορισμού κοινών όρων, μεθόδους και τεχνικές αναγνώρισης ταυτότητας και για την κατάρτιση ενός κοινού εντύπου για τις αιτήσεις εγκληματολογικής έρευνας. Η Ευρωπαϊκή Ένωση θα πρέπει να συμμετάσχει σε αυτές τις εργασίες, τόσο στο επίπεδο των οργανισμών των κρατών μελών που είναι εξειδικευμένοι στις έρευνες για τα εγκλήματα πληροφορικής όσο και στο επίπεδο της έρευνας και ανάπτυξης που χρηματοδοτείται από το 5^{ο} πρόγραμμα πλαίσιο (πρόγραμμα ΤΚΠ).

6. ΜΗ ΝΟΜΟΘΕΤΙΚΑ ΜΕΤΡΑ

Η εφαρμογή κατάλληλης νομοθεσίας σε εθνικό και διεθνές επίπεδο είναι απαραίτητη, αλλά δεν επαρκεί από μόνη της για να καταπολεμηθούν αποτελεσματικά τα εγκλήματα πληροφορικής και η δόλια χρήση των δικτύων. Είναι απαραίτητο εξίσου να υπάρχουν και άλλες μη νομοθετικές προϋποθέσεις που να συμπληρώνουν το νομοθετικό πλαίσιο. Ορισμένες εξ αυτών περιλαμβάνονται στις συστάσεις της μελέτης COMCRIME, ενώ η

---

60 COM(2000) 495, Βρυξέλλες 26.7.2000.

ομάδα των χωρών G8 πρότεινε παρόμοιες προϋποθέσεις στο σχέδιο δράσης σε 10 σημεία και αυτές έχουν τύχει ευρείας υποστήριξης από όλους τους συμμετέχοντες στην άτυπη διαδικασία διαβούλευσης που προηγήθηκε της σύνταξης της παρούσας κοινοποίησης. Αυτές οι προϋποθέσεις περιλαμβάνουν:

- τη δημιουργία εξειδικευμένων στα εγκλήματα πληροφορικής αστυνομικών μονάδων, εκεί όπου αυτές δεν υπάρχουν ήδη·

- τη βελτίωση της συνεργασίας μεταξύ των οργάνων εφαρμογής του νόμου, των επιχειρήσεων, των οργανώσεων καταναλωτών και των αρχών που είναι επιφορτισμένες με την προστασία των δεδομένων·

- μέτρα με σκοπό να ενθαρρυνθούν οι επιχειρήσεις και οι οργανώσεις πολιτών να αναλαμβάνουν κατάλληλες πρωτοβουλίες, συμπεριλαμβανομένης της ασφάλειας των προϊόντων.

Το θέμα της κρυπτογράφησης φαίνεται να παραμένει σημαντικό στο συγκεκριμένο πλαίσιο. Πρόκειται για απαραίτητο εργαλείο για να διευκολύνει την εφαρμογή και την έγκριση νέων υπηρεσιών, συμπεριλαμβανομένου του ηλεκτρονικού εμπορίου και μπορεί να διαδραματίσει σημαντικό ρόλο στην πρόληψη εγκληματικών πράξεων στο Διαδίκτυο. Η πολιτική της Επιτροπής στο θέμα της κρυπτογράφησης έχει αναλυθεί στην ανακοίνωσή της του 1997[61] για την κατοχύρωση ασφάλειας και εμπιστοσύνης στις ηλεκτρονικές επικοινωνίες, στην οποία η Επιτροπή όριζε ότι θα καταβάλει προσπάθειες για την άρση όλων των περιορισμών στην ελεύθερη κυκλοφορία όλων των προϊόντων κρυπτογράφησης στο επίπεδο της Ευρωπαϊκής Κοινότητας. Η ανακοίνωση ορίζει εξάλλου ότι οι εθνικοί περιορισμοί στην ελεύθερη κυκλοφορία των προϊόντων κρυπτογράφησης πρέπει να συμβιβάζονται με το κοινοτικό δίκαιο και ότι η Επιτροπή θα εξετάσει το κατά πόσον αυτοί οι εθνικοί περιορισμοί είναι δικαιολογημένοι και ανάλογοι, κυρίως σε σχέση με τις διατάξεις της συνθήκης που αφορούν την ελεύθερη κυκλοφορία, τη νομολογία του Δικαστηρίου και τις αξιώσεις των οδηγιών για την προστασία των δεδομένων. Εντούτοις, η Επιτροπή αναγνωρίζει ότι η κρυπτογράφηση δημιουργεί επίσης νέα και δύσκολα προβλήματα για τα όργανα εφαρμογής του νόμου.

Η Επιτροπή ως εκ τούτου καλωσορίζει τον πρόσφατα εγκριθέντα κανονισμό για τα αγαθά διπλής χρήσης, ο οποίος συνέβαλε στην απελευθέρωση της πρόσβασης στα προϊόντα κρυπτογράφησης, παραδεχόμενη παράλληλα ότι αυτές οι ανάγκες πρέπει να συνοδεύονται από βελτιωμένο διάλογο μεταξύ χρηστών, βιομηχανίας και αρχών εφαρμογής του νόμου. Από την πλευρά της, η Επιτροπή προτίθεται να προωθήσει αυτόν τον διάλογο σε ευρωπαϊκό επίπεδο μέσω του προτεινόμενου φόρουμ της ΕΕ για το έγκλημα υψηλής τεχνολογίας. Η διάδοση σε μεγάλη κλίμακα προϊόντων ασφαλείας στο σύνολο της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένων των προϊόντων υψηλής κρυπτογράφησης, επικυρωμένων, εφόσον χρειάζεται, βάσει κοινά αποδεκτών κριτηρίων αξιολόγησης, θα ενίσχυε ταυτόχρονα τις δυνατότητες πρόληψης εγκληματικών πράξεων και την εμπιστοσύνη των χρηστών στις τεχνικές της κοινωνίας της πληροφορίας.

6.1. Εξειδικευμένες μονάδες σε εθνικό επίπεδο

Δεδομένης της νομικής και τεχνικής πολυπλοκότητας ορισμένων εγκληματικών πράξεων στον τομέα της πληροφορικής, είναι απαραίτητο να δημιουργηθούν εξειδικευμένες μονάδες σε εθνικό επίπεδο. Αυτές οι πολυθεματικές μονάδες (αρχές εφαρμογής του νόμου και

---

61 COM(97)503.

δικαστικές αρχές), εφοδιασμένες με κατάλληλα καταρτισμένο προσωπικό, θα πρέπει να είναι εξοπλισμένες με κατάλληλες τεχνικές εγκαταστάσεις και να λειτουργούν ως ταχέα σημεία επαφής, προκειμένου:

- να ανταποκρίνονται ταχέως στις αιτήσεις πληροφοριών για εικαζόμενες παραβάσεις. Θα πρέπει να καθοριστούν κοινά μορφότυπα για την ανταλλαγή τέτοιων πληροφοριών, αν και οι συζητήσεις των εμπειρογνωμόνων της ομάδας G8 απέδειξαν ότι οι εθνικές διαφορές στο νομικό τομέα ενδέχεται να καταστήσουν δύσκολο αυτό το καθήκον·

- να δρουν ως μονάδες διασύνδεσης σε εθνικό και διεθνές επίπεδο για ανοικτές τηλεφωνικές γραμμές[62] και να δέχονται καταγγελίες για παράνομο περιεχόμενο εκ μέρους χρηστών του Διαδικτύου·

- να βελτιώνουν και να αναπτύσσουν εξειδικευμένες τεχνικές στον τομέα της ηλεκτρονικής έρευνας, προκειμένου να εντοπίζουν τα εγκλήματα πληροφορικής, να διεξάγουν τις σχετικές έρευνες και να ασκούν διώξεις·

- να δρουν ως κέντρο αριστείας για τα θέματα των εγκλημάτων πληροφορικής προκειμένου να συμμερίζονται τις βέλτιστες πρακτικές και εμπειρίες.

Στο πλαίσιο της Ευρωπαϊκής Ένωσης, ορισμένα κράτη μέλη, έχουν ήδη θέσει σε λειτουργία αυτές τις εξειδικευμένες μονάδες που ασχολούνται με τα εγκλήματα πληροφορικής. Η Επιτροπή θεωρεί ότι η δημιουργία αυτών των μονάδων υπάγεται στην αρμοδιότητα των κρατών μελών και ενθαρρύνει έντονα αυτά τα τελευταία να λαμβάνουν μέτρα προς αυτή την κατεύθυνση. Το κόστος που συνεπάγεται η αγορά προσφάτων συστημάτων εξοπλισμού και λογισμικού για αυτές τις μονάδες καθώς και η κατάρτιση του προσωπικού τους είναι σημαντικό και αυτό προϋποθέτει εκ των προτέρων ότι οι δημόσιες αρχές καθορίζουν προτεραιότητες και λαμβάνουν πολιτικές αποφάσεις στο επίπεδο που αρμόζει.[63] Η εμπειρία των ήδη υφιστάμενων μονάδων σε ορισμένα κράτη μέλη θα μπορούσε να αποδειχθεί ιδιαίτερα πολύτιμη και η Επιτροπή θα λάβει τα απαραίτητα μέτρα για να ενθαρρύνει τις ανταλλαγές στο συγκεκριμένο τομέα.

Η Επιτροπή θεωρεί επίσης ότι η Europol μπορεί να παράσχει περαιτέρω προστιθέμενη αξία σε κοινοτικό επίπεδο, μέσω του συντονισμού, της ανάλυσης και άλλων μορφών βοήθειας στις εθνικές εξειδικευμένες μονάδες. Η Επιτροπή θα υποστηρίξει συνεπώς την επέκταση της εντολής της Europol στα εγκλήματα πληροφορικής.

---

62 Μέχρι σήμερα, ανοικτές τηλεφωνικές γραμμές υπήρχαν μόνο σε περιορισμένο αριθμό χωρών. Μεταξύ αυτών, η Cybertipline στις Ηνωμένες Πολιτείες και το Internet Watch Foundation (IWF) στο ΗΒ, το οποίο έθεσε σε λειτουργία, από το Δεκέμβριο 1996, ανοικτή τηλεφωνική γραμμή και ηλεκτρονικό ταχυδρομείο προκειμένου οι χρήστες να επισημαίνουν τα έγγραφα που συνάντησαν στο Διαδίκτυο, τα οποία θεωρούν παράνομα. Το IWF αποφασίζει για τον παράνομο χαρακτήρα του εγγράφου, ενημερώνει τους παρόχους υπηρεσιών διαδικτύου και την αστυνομία. Άλλοι οργανισμοί ελέγχου υπάρχουν επίσης στη Νορβηγία (Redd Barna), στις Κάτω Χώρες (Meldpunt), στη Γερμανία (Newswatch, FSM και Jugendschutz), στην Αυστρία (ISPAA) και στην Ιρλανδία (ISPAI). Στο πλαίσιο του κοινοτικού προγράμματος Daphne, η Childnet International εφαρμόζει τώρα ένα σχέδιο άμεσα σχετιζόμενο με το συγκεκριμένο ζήτημα ("International Hotline Providers in Europe Forum"). Επίσης, οι εμπειρογνώμονες της UNESCO που συνήλθαν στο Παρίσι τον Ιανουαρίου 1999 υποστήριξαν και ενθάρρυναν τη δημιουργία εθνικών ανοιχτών τηλεφωνικών γραμμών, τη δημιουργία δικτύων ανοικτών τηλεφωνικών γραμμών ή ενός διεθνούς "ηλεκτρονικού παρατηρητηρίου".

63 Όσον αφορά την αμερικανική εμπειρία στο συγκεκριμένο τομέα, βλέπε Michael A. Sussmann “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium”, Duke Journal of Comparative and International Law, Τόμος. 9 Άνοιξη 1999, σ. 464.

6.2. Εξειδικευμένη κατάρτιση

Απαιτείται σημαντική προσπάθεια στον τομέα της συνεχούς, εξειδικευμένης κατάρτισης του αστυνομικού και δικαστικού προσωπικού. Οι τεχνικές και οι ικανότητες στον τομέα των εγκλημάτων πληροφορικής αλλάζουν ταχύτερα από τους πιο κλασσικούς τομείς εγκληματικής δραστηριότητας.

Ορισμένα κράτη μέλη έχουν εφαρμόσει πρωτοβουλίες για να καταρτίσουν το προσωπικό των αρχών εφαρμογής του νόμου στις προηγμένες τεχνολογίες. Θα μπορούσαν να παρέχουν συμβουλές και προσανατολισμούς στα κράτη μέλη που δεν έχουν ακόμα λάβει παρόμοια μέτρα.

Διάφορα σχέδια προς αυτή την κατεύθυνση, υπό τη μορφή ανταλλαγής πληροφοριών, σεμιναρίων για τις κοινές προκλήσεις που αντιμετωπίζονται από τις σχετικές επαγγελματικές κατηγορίες, έχουν ξεκινήσει με την υποστήριξη προγραμμάτων που διευθύνονται από την Επιτροπή (ιδιαίτερα τα προγράμματα STOP, FALCONE και GROTIUS). Η Επιτροπή θα προτείνει περισσότερες δραστηριότητες στο συγκεκριμένο τομέα, κυρίως όσον αφορά την κατάρτιση στον τομέα της πληροφορικής και της απευθείας σύνδεσης.

Η Europol ανέλαβε την πρωτοβουλία να πραγματοποιήσει, το Νοέμβριο 2000, μια συνεδρίαση κατάρτισης μια εβδομάδας απευθυνόμενη στο προσωπικό των αρχών εφαρμογής του νόμου των κρατών μελών, η οποία θα έχει ως κύριο θέμα την παιδική πορνογραφία. Το πεδίο μιας τέτοιας συνεδρίασης θα μπορούσε να επεκταθεί ώστε να συμπεριλάβει τα εγκλήματα πληροφορικής εν γένει. Η Interpol είναι επίσης παρούσα στο συγκεκριμένο τομέα εδώ και πολλά έτη. Θα μπορούσε να επιδιώξει τη συμμετοχή περισσοτέρων ατόμων στις πρωτοβουλίες της που αφορούν το συγκεκριμένο θέμα.

Η ομάδα G8 διοργάνωσε δραστηριότητες που επιτρέπουν την ανταλλαγή εμπειριών μεταξύ αρχών εφαρμογής του νόμου και την επεξεργασία κοινών τεχνικών έρευνας με βάση συγκεκριμένες περιπτώσεις. Συμπληρωματική δράση στον τομέα της κατάρτισης θα πρέπει να ξεκινήσει κατά το δεύτερο εξάμηνο του 2001. Τα κράτη μέλη της Ευρωπαϊκής Ένωσης που αποτελούν συμβαλλόμενα μέρη της ομάδας G8 θα μπορούσαν να συμμεριστούν αυτές τις εμπειρίες με τα άλλα κράτη μέλη.

Στο συγκεκριμένο τομέα της καταπολέμησης της παιδικής πορνογραφίας στο Διαδίκτυο, η δημιουργία και η διαχείριση, σε διεθνές επίπεδο, μιας κεντρικής ψηφιακής βιβλιοθήκης με εικόνες παιδικής πορνογραφίας σε διεθνές επίπεδο (η οποία θα μπορεί να διατίθεται στο Διαδίκτυο για τις εξειδικευμένες μονάδες εφαρμογής του νόμου σε εθνικό επίπεδο, τηρώντας τις απαραίτητες προϋποθέσεις και περιορισμούς όσον αφορά την πρόσβαση και την προστασία του ιδιωτικού βίου) θα διευκόλυνε την έρευνα θυμάτων και δραστών, θα συντελούσε στον προσδιορισμό του χαρακτήρα των αδικημάτων και στην κατάρτιση εξειδικευμένων αστυνομικών υπαλλήλων.[64]

---

[64] Στο συγκεκριμένο πλαίσιο, το σχέδιο "Excalibur" το οποίο αναπτύχθηκε από τη σουηδική National Crime Intelligence Division και υποστηρίζεται από την Ευρωπαϊκή Επιτροπή στο πλαίσιο του προγράμματος STOP, είχε πολύ καλά αποτελέσματα. Αυτή η πρωτοβουλία τέθηκε σε εφαρμογή σε συνεργασία με τις γερμανικές, βρετανικές, ολλανδικές και βελγικές αστυνομικές δυνάμεις, από κοινού με την Europol και την Interpol. Ελήφθησαν επίσης υπόψη άλλα σχέδια που έχουν αναπτυχθεί από την γερμανική BKA (το "Perkeo") και το γαλλικό Υπουργείο Εσωτερικών (σχέδιο"Surfimage", που επίσης υποστηρίζεται στο πλαίσιο του προγράμματος STOP).

6.3. Βελτιωμένη πληροφόρηση και κοινοί κανόνες για την τήρηση αρχείων

Η δημιουργία εναρμονισμένων κανόνων για την αστυνομική και δικαστική τήρηση αρχείων και κατάλληλων εργαλείων για στατιστική ανάλυση των εγκλημάτων πληροφορικής θα βοηθούσε τις αρχές εφαρμογής του νόμου και τις δικαστικές αρχές να βελτιώσουν την αποθήκευση, ανάλυση και αξιολόγηση των επίσημων πληροφοριών που συγκεντρώνονται στο συγκεκριμένο συνεχώς μεταβαλλόμενο τομέα.

Επίσης, από την άποψη του ιδιωτικού τομέα, αυτές οι στατιστικές είναι απαραίτητες για να αξιολογηθούν ορθά οι ενυπάρχοντες κίνδυνοι και να αναλυθεί η σχέση κόστους/ωφελειών της διαχείρισής τους. Πρόκειται για σημαντικό θέμα, όχι μόνο για λειτουργικούς λόγους (για να αποφασισθεί, για παράδειγμα, το είδος μέτρων ασφαλείας που πρέπει να ληφθούν) αλλά και για λόγους ασφάλειας.

Μια βάση δεδομένων που περιλαμβάνει τα νομοθετικά κείμενα για τα εγκλήματα πληροφορικής, η οποία αποτελούσε μέρος της μελέτης COMCRIME, ευρίσκεται στο στάδιο της ενημέρωσης και θα τεθεί στη διάθεση της Επιτροπής. Η Επιτροπή θα εξετάσει τη βελτίωση του περιεχομένου (συμπεριλαμβάνοντας νομοθετικά κείμενα, νομολογία και δημοσιεύσεις) και της χρηστικότητας της βάσης δεδομένων.

6.4. Συνεργασία μεταξύ των διαφόρων φορέων: το φόρουμ της Ευρωπαϊκής Ένωσης

Η ύπαρξη αποτελεσματικής συνεργασίας μεταξύ των δημοσίων αρχών και των επιχειρήσεων, στο εσωτερικό του νομικού πλαισίου, θεωρείται θεμελιώδες στοιχείο κάθε δημόσιας πολιτικής που αποβλέπει στην καταπολέμηση του εγκλήματος πληροφορικής.[65] Οι αντιπρόσωποι των αρχών εφαρμογής του νόμου παραδέχθηκαν ότι στερούντο ενίοτε σαφήνειας και ακρίβειας για να προσδιορίσουν στους παρόχους υπηρεσιών αυτό που πραγματικά χρειάζονταν. Οι αντιπρόσωποι των επιχειρήσεων επέδειξαν στο σύνολό τους θετική στάση για τη βελτίωση της συνεργασίας με τις αρχές εφαρμογής του νόμου, ενώ τονίσθηκε η ανάγκη να εξευρεθεί εύλογη ισορροπία μεταξύ της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των πολιτών, κυρίως του δικαιώματος τους στον ιδιωτικό βίο,[66] της ανάγκης καταπολέμησης της εγκληματικότητας και των οικονομικών επιβαρύνσεων που επιβάλλονται στους φορείς παροχής.

---

65 Στο ανακοινωθέν που εξεδόθη στην Ουάσινγκτον στις 9 και 10 Δεκεμβρίου 1997 για τις αρχές και τα 10 σημεία δράσης για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας, οι Υπουργοί Δικαιοσύνης και Εσωτερικών Υποθέσεων της ομάδας G8 δήλωσαν ότι: ΄"είναι οι επιχειρήσεις αυτές που σχεδιάζουν, χρησιμοποιούν και διαχειρίζονται αυτά τα παγκόσμια δίκτυα και είναι οι κύριοι υπεύθυνοι για την ανάπτυξη τεχνικών προδιαγραφών. Επαφίεται συνεπώς σε αυτές να διαδραματίσουν το ρόλο τους στην επεξεργασία και διανομή συστημάτων ασφαλείας που σχεδιάζονται για να βοηθήσουν τη διερεύνηση καταχρηστικών χρήσεων ηλεκτρονικών δεδομένων, στη διατήρηση ηλεκτρονικών αποδείξεων και στη διευκόλυνση του εντοπισμού και του προσδιορισμού της ταυτότητας των εγκληματιών". Η απόφαση του Συμβουλίου για την καταπολέμηση της παιδικής πορνογραφίας στο Διαδίκτυο τονίζει την ανάγκη που υπάρχει για τα κράτη μέλη να ξεκινήσουν εποικοδομητικό διάλογο με τις επιχειρήσεις και να συνεργαστούν μαζί τους συμμεριζόμενα τις εμπειρίες τους.

66 Όπως ορίζεται στις κοινοτικές οδηγίες σχετικά με την προστασία των δεδομένων, στη σύμβαση του Συμβουλίου της Ευρώπης για τα δικαιώματα του ανθρώπου στη σύμβαση του Συμβουλίου της Ευρώπης αριθ. 108 για την προστασία των προσώπων από την αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα και στο αντίστοιχο εθνικό δίκαιο.

Οι επιχειρήσεις και οι αρχές εφαρμογής του νόμου μπορούν, συνδυάζοντας τις προσπάθειές τους, να ευαισθητοποιήσουν το κοινό για τους κινδύνους που αντιπροσωπεύουν οι εγκληματίες στο Διαδίκτυο, να ενθαρρύνουν τις βέλτιστες πρακτικές στον τομέα της ασφάλειας και να επεξεργαστούν αποτελεσματικά μέσα και διαδικασίες για την καταπολέμηση της εγκληματικότητας. Πρωτοβουλίες προς αυτή την κατεύθυνση έχουν ήδη αναληφθεί από ορισμένα κράτη μέλη, εκ των οποίων η παλαιότερη και πιο φιλόδοξη είναι αναμφίβολα το βρετανικό Internet Crime Forum.[67]

Η Επιτροπή καλωσορίζει αυτές τις πρωτοβουλίες και θεωρεί ότι αυτές θα πρέπει να ενθαρρυνθούν σε όλα τα κράτη μέλη. Η Επιτροπή προτίθεται να δημιουργήσει ένα φόρουμ που θα συγκεντρώνει τις αρχές εφαρμογής του νόμου, τους φορείς παροχής υπηρεσιών Διαδικτύου, του φορείς τηλεπικοινωνιών, τις οργανώσεις πολιτικών ελευθεριών, τους αντιπροσώπους καταναλωτών, τις αρχές για την προστασία δεδομένων, και άλλους ενδιαφερόμενους με σκοπό να εντατικοποιήσει τη συνεργασία σε κοινοτικό επίπεδο. Σε μια πρώτη φάση, αυτό το φόρουμ θα περιλαμβάνει δημόσιους υπαλλήλους που θα διοριστούν από τα κράτη μέλη, εμπειρογνώμονες στον τομέα της τεχνολογίας και της προστασίας του ιδιωτικού βίου που θα διοριστούν από την ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων και αντιπροσώπους της βιομηχανίας και των καταναλωτών που θα προσδιοριστούν σε στενή συνεργασία με τις ενώσεις βιομηχανίας και καταναλωτών. Σε μεταγενέστερη φάση, αυτό το φόρουμ θα περιλαμβάνει αντιπροσώπους από αντίστοιχες εθνικές πρωτοβουλίες.

Το φόρουμ της Ευρωπαϊκής Ένωσης θα λειτουργεί με ανοιχτό και διαφανή τρόπο και τα σχετικά έγγραφα θα δημοσιεύονται στο Διαδίκτυο επιτρέποντας την υποβολή σχολίων εκ μέρους των ενδιαφερομένων μερών.

Το φόρουμ θα κληθεί να εξετάσει ιδιαίτερα τους ακόλουθους τομείς :

- Ανάπτυξη, όπου χρειάζεται, σημείων επαφής που θα λειτουργούν όλο το 24ωρο μεταξύ των δημοσίων αρχών και των επιχειρήσεων·

- Ανάπτυξη τυποποιημένου μορφοτύπου για τις αιτήσεις πληροφοριών που απευθύνονται από τις αρχές εφαρμογής του νόμου στις επιχειρήσεις και ενίσχυση της χρήσης του Διαδικτύου από τις αρχές εφαρμογής του νόμου όταν επικοινωνούν με τους φορείς παροχής υπηρεσιών·

- Ενθάρρυνση της επεξεργασίας και εφαρμογής κωδίκων συμπεριφοράς και βέλτιστων πρακτικών και διανομή μεταξύ επιχειρήσεων και δημοσίων αρχών[68]·

- Ενθάρρυνση της ανταλλαγής πληροφοριών για τις τάσεις που υπάρχουν στον τομέα του εγκλήματος υψηλής τεχνολογίας μεταξύ των διαφόρων μερών, ειδικότερα των επιχειρήσεων και των αρχών εφαρμογής του νόμου·

---

67 Το Internet Crime Forum, το οποίο δημιουργήθηκε το 1997, συγκεντρώνει αστυνομικούς υπαλλήλους, υπαλλήλους του βρετανικού Υπουργείου Εσωτερικών, υπευθύνους για την προστασία των δεδομένων και αντιπροσώπους του τομέα του Διαδικτύου· αυτό το φόρουμ πραγματοποιεί ολομέλειες τρεις ή τέσσερις φορές κατ΄ έτος και διαθέτει ορισμένες μόνιμες ομάδες εργασίας.

68 Στο μέτρο που πρόκειται για κώδικες συμπεριφοράς κατά την έννοια του άρθρου 27 της οδηγίας 95/46/ΕΚ (θα μπορούσαν για παράδειγμα να εξετάζουν ζητήματα που άπτονται της οδηγίας 97/66/ΕΚ, όπως οι παρακολουθήσεις συνδιαλέξεων), συμμετέχουν η ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων και οι εθνικές αρχές ελέγχου που είναι επιφορτισμένες με την προστασία δεδομένων.

- Εξέταση των προβληματισμών των αρχών εφαρμογής του νόμου για την ανάπτυξη των νέων τεχνολογιών·

- Ενθάρρυνση της περαιτέρω ανάπτυξης των μηχανισμών έγκαιρης προειδοποίησης και διαχείρισης κρίσεων για να προληφθούν, προσδιοριστούν και αναλυθούν οι απειλές ή οι διαταραχές που λαμβάνουν χώρα στις ηλεκτρονικές υποδομές·

- Εξασφάλιση, ανάλογα με τις ανάγκες, προστιθέμενης αξίας, από την άποψη εμπειρογνωμοσύνης, στις εργασίες που διεξάγονται στο πλαίσιο του Συμβουλίου και άλλων διεθνών φόρουμ, όπως το Συμβούλιο της Ευρώπης και η ομάδα των 8·

- Ενθάρρυνση της συνεργασίας των ενδιαφερομένων μερών, συμπεριλαμβανομένων των αρχών που γίνονται δεκτές με κοινή συμφωνία από τις αρχές εφαρμογής του νόμου, τις επιχειρήσεις και τους χρήστες (π.χ. Μνημόνιο Συμφωνίας, Κώδικες Δεοντολογίας σύμφωνα με το νομικό πλαίσιο).

6.5. Ενέργειες που διεξάγονται άμεσα από τις επιχειρήσεις

Η καταπολέμηση του εγκλήματος πληροφορικής είναι, σε μεγάλο βαθμό, προς το συμφέρον της ευρύτερης κοινωνίας. Εφόσον επιδιώκεται η εμπιστοσύνη των καταναλωτών στο ηλεκτρονικό εμπόριο, τα μέτρα πρόληψης του εγκλήματος πληροφορικής πρέπει να γίνουν δεκτά ως στοιχείο καλής εμπορικής πρακτικής. Πολλοί οικονομικοί τομείς, όπως οι τράπεζες, οι ηλεκτρονικές επικοινωνίες, οι οργανισμοί πιστωτικών καρτών και δικαιωμάτων πνευματικής ιδιοκτησίας, καθώς και οι πελάτες τους, αποτελούν δυνάμει θύματα του εγκλήματος πληροφορικής. Οι εταιρείες προστατεύουν βέβαια τις δικές τους εμπορικές επωνυμίες και σήματα και διαδραματίζουν κατά συνέπεια ρόλο στην πρόληψη της απάτης. Ορισμένοι οργανισμοί που εκπροσωπούν τους τομείς λογισμικού και ήχου (π.χ., British Phonographic Industry - BPI) διαθέτουν ομάδες επιφορτισμένες με τις έρευνες πειρατείας (συμπεριλαμβανομένου του Διαδικτύου). Σε ορισμένα κράτη μέλη, οι πάροχοι υπηρεσιών στο Διαδίκτυο έχουν θέσει σε λειτουργία απευθείας τηλεφωνικές γραμμές που επιτρέπουν στους χρήστες να επισημαίνουν τα μηνύματα με παράνομο και επιζήμιο περιεχόμενο.

Η Επιτροπή έχει υποστηρίξει ορισμένες από αυτές τις πρωτοβουλίες ενθαρρύνοντας τη συμμετοχή τους στο κοινοτικό πρόγραμμα πλαίσιο έρευνας και ανάπτυξης, στο Internet Action Plan[69] και στα προγράμματα του τίτλου VI όπως STOP και DAPHNE.

Το φόρουμ θα επιτρέψει την ανταλλαγή των βέλτιστων πρακτικών στους συγκεκριμένους τομείς.

6.6. Σχέδια έρευνας και τεχνολογικής ανάπτυξης (ΕΤΑ) που χρηματοδοτούνται από την Ευρωπαϊκή Ένωση

Το πρόγραμμα ΕΤΑ για τις τεχνολογίες της κοινωνίας της πληροφορίας (ΤΚΠ), το οποίο αποτελεί τμήμα του 5ου Προγράμματος πλαισίου (1998 έως 2002), δίνει έμφαση στην ανάπτυξη και χρήση τεχνολογιών οικοδόμησης εμπιστοσύνης. Οι τεχνολογίες οικοδόμησης εμπιστοσύνης περιλαμβάνουν ταυτόχρονα την ασφάλεια των πληροφοριών και των δικτύων, καθώς και τεχνικά μέσα και μεθόδους για την προστασία έναντι παραβιάσεων των

---

[69] Περισσότερες πληροφορίες για το Internet Action Plan: σχέδιο δράσης για την προώθηση της ασφαλέστερης χρήσης του δικτύου στην ηλεκτρονική διεύθυνση http://158.169.50.95:10080/iap/.

θεμελιωδών δικαιωμάτων προστασίας του ιδιωτικού βίου και των δεδομένων και άλλων ατομικών δικαιωμάτων και για την καταπολέμηση του εγκλήματος πληροφορικής.

Το πρόγραμμα ΤΚΠ, και ειδικότερα οι εργασίες που αφορούν την *ασφάλεια πληροφοριών και δικτύων και άλλες τεχνολογίες οικοδόμησης εμπιστοσύνης* στη Κεντρική Δράση 2 - *Νέες μέθοδοι εργασίας και ηλεκτρονικό εμπόριο*, προβλέπει πλαίσιο που παρέχει τη δυνατότητα να αναπτυχθούν ικανότητες και τεχνολογίες για την κατανόηση και την αντιμετώπιση των νέων τεχνολογικών προκλήσεων που έχουν σχέση με την πρόληψη και την καταστολή του εγκλήματος πληροφορικής και να κατοχυρωθεί ότι οι αξιώσεις ασφάλειας και προστασίας του ιδιωτικού βίου μπορούν να πληρούνται στο επίπεδο της Ευρωπαϊκής Ένωσης, των ιδεατών κοινοτήτων και του ατόμου.

Επιπλέον προκειμένου να αντιμετωπιστούν κατάλληλα αυτά τα προβλήματα εμπιστοσύνης συμπεριλαμβανομένης της πρόληψης και της διερεύνησης του εγκλήματος πληροφορικής, ανελήφθη πρωτοβουλία σχετικά με την ασφάλεια στο πλαίσιο του προγράμματος ΤΚΠ. Η πρωτοβουλία αυτή στοχεύει στο να ενισχύσει και να κατοχυρώσει την εμπιστοσύνη στις ισχυρά διασυνδεδεμένες ηλεκτρονικές υποδομές και στα ενσωματωμένα συστήματα που λειτουργούν στενά σε δίκτυο, ενθαρρύνοντας την ευαισθητοποίηση όσον αφορά τα προβλήματα ασφάλειας και τεχνολογίες που επιτρέπουν την επίτευξή της. Η διεθνής συνεργασία αποτελεί επίσης μέρος αυτής της πρωτοβουλίας. Το πρόγραμμα (ΤΚΠ) έχει αναπτύξει σχέσεις εργασίας με τις υπηρεσίες των ΗΠΑ DARPA (υπηρεσία έργων προηγμένης έρευνας στο πεδίο της άμυνας) και NSF (Εθνικό Ίδρυμα για τις Επιστήμες) και έχει δημιουργήσει, σε συνεργασία με το Υπουργείο Εξωτερικών, την κοινή Task Force για την προστασία των υποδομών ζωτικής σημασίας, υπό την αιγίδα της κοινής ΕΚ/ΗΠΑ συμβουλευτικής ομάδας της συμφωνίας επιστημονικής και τεχνολογικής συνεργασίας.[70]

Το Κοινό Κέντρο Έρευνας της Επιτροπής (ΚΚΕΕ), το οποίο υποστηρίζει την πρωτοβουλία για την ασφάλεια λειτουργίας στο πλαίσιο του προγράμματος ΤΚΠ, θα επικεντρώσει τις προσπάθειές του στην ανάπτυξη κατάλληλων και εναρμονισμένων μέτρων, δεικτών και στατιστικών σε διαβούλευση με τα άλλα ενδιαφερόμενα μέρη και την Europol. Σκοπός θα είναι να ταξινομηθούν και να κατανοηθούν ορθά οι παράνομες δραστηριότητες, η γεωγραφική κατανομή τους, οι ρυθμοί εξέλιξής τους και η αποτελεσματικότητα των δράσεων που αναλαμβάνονται για την καταπολέμησή τους. Το ΚΚΕΕ θα καλέσει, εφόσον χρειάζεται, άλλες ομάδες έρευνας και θα χρησιμοποιήσει τις εργασίες τους και τα αποτελέσματά τους. Θα διατηρεί θέση στο Διαδίκτυο σχετικά με αυτό το θέμα και θα αναφέρει τις προόδους που σημειώνει στο συγκεκριμένο θέμα στο φόρουμ της Ευρωπαϊκής Ένωσης.

7. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

Για την πρόληψη του εγκλήματος πληροφορικής και την αποτελεσματική καταπολέμηση αυτού του φαινομένου απαιτείται η προηγούμενη ύπαρξη ορισμένων προϋποθέσεων:

- διαθεσιμότητα τεχνολογιών στον τομέα της πρόληψης. Αυτό προϋποθέτει κατάλληλο κανονιστικό πλαίσιο το οποίο αφήνει το πεδίο ελεύθερο στην καινοτομία και στην έρευνα και τις ενθαρρύνει. Η προσφυγή στη δημόσια χρηματοδότηση μπορεί να θεωρηθεί δικαιολογημένη για να υποστηριχθεί η ανάπτυξη και η χρησιμοποίηση τεχνολογιών κατάλληλης προστασίας·

[70] Περισσότερες πληροφορίες για το πρόγραμμα ΤΚΠ διατίθενται στη διεύθυνση http://www.cordis.lu/ist.

- ευαισθητοποίηση στους ενδεχόμενους κινδύνους που έχουν σχέση με την ασφάλεια και στα μέσα καταπολέμησής τους·

- κατάλληλες νομοθετικές διατάξεις στον τομέα του ουσιαστικού και δικονομικού δικαίου, όσον αφορά τις εθνικές και διεθνείς εγκληματικές δραστηριότητες. Στο επίπεδο του ποινικού δικαίου, οι εθνικές νομοθεσίες θα πρέπει να είναι επαρκώς λεπτομερείς και αποτελεσματικές για να τιμωρούν τα σοβαρά εγκλήματα πληροφορικής και να προβλέπουν αποτρεπτικές κυρώσεις, να συμβάλλουν στην επίλυση των προβλημάτων που θέτει το διπλό αξιόποινο[71] και να διευκολύνουν τη διεθνή συνεργασία. Όταν υπάρχει πλήρως δικαιολογημένη ανάγκη δράσης των υπηρεσιών εφαρμογής του νόμου ώστε να αναζητούν, κατάσχουν και αντιγράφουν ασφαλώς δεδομένα πληροφορικής στο εσωτερικό της επικράτειάς τους, προκειμένου να μπορούν να διεξάγουν έρευνες για εγκλήματα πληροφορικής, το δικονομικό δίκαιο θα πρέπει να το επιτρέπει, σύμφωνα με τις αρχές και τις εξαιρέσεις που προβλέπονται από το κοινοτικό δίκαιο και από την Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων. Η Επιτροπή πιστεύει ότι η συμφωνία που επιτεύχθηκε όσον αφορά τις διατάξεις που διέπουν την παρακολούθηση συνδιαλέξεων στο πλαίσιο της σύμβασης για την αμοιβαία δικαστική συνδρομή σε ποινικές υποθέσεις αντιπροσωπεύει το ανώτατο όριο το οποίο μπορεί να επιτευχθεί επί του παρόντος. Η Επιτροπή θα συνεχίσει να ελέγχει την εφαρμογή, με τη βοήθεια των κρατών μελών, των επιχειρήσεων και των χρηστών, προκειμένου να κατοχυρώσει ότι οι αντίστοιχες πρωτοβουλίες θα είναι αποτελεσματικές, διαφανείς και ισορροπημένες·

- διαθεσιμότητα επαρκούς, καλά καταρτισμένου και εξοπλισμένου προσωπικού για την εφαρμογή του νόμου. Η στενή συνεργασία με τους παρόχους υπηρεσιών Διαδικτύου και τους φορείς τηλεπικοινωνιών στον τομέα της κατάρτισης θα ενθαρρυνθεί ιδιαιτέρως·

- ενίσχυση της συνεργασίας μεταξύ όλων των σχετικών φορέων: χρήστες, καταναλωτές, επιχειρήσεις, αρχές εφαρμογής του νόμου και αρχές προστασίας δεδομένων. Αυτή η προϋπόθεση είναι ουσιαστική για τις έρευνες που αφορούν τα εγκλήματα πληροφορικής και για την προστασία της δημόσιας ασφάλειας. Είναι απαραίτητο να καθοριστούν με σαφήνεια οι κανόνες και οι υποχρεώσεις που διέπουν τη δραστηριότητα των επιχειρήσεων. Οι δημόσιες αρχές πρέπει να αναγνωρίσουν ότι οι ανάγκες εφαρμογής του νόμου μπορούν να επιβάλλουν βάρη στις επιχειρήσεις και, κατά συνέπεια, να λάβουν εύλογα μέτρα για τη μείωση αυτών των βαρών. Παράλληλα, οι επιχειρήσεις θα πρέπει να ενσωματώσουν στις εμπορικές τους πρακτικές προβληματισμούς δημόσιας ασφάλειας. Η ενεργή συνεργασία και υποστήριξη του μεμονωμένου χρήστη και καταναλωτή θα καταστούν σε σχέση με το θέμα αυτό ολοένα και πιο αναγκαίες·

- συνεχείς πρωτοβουλίες της βιομηχανίας και των τοπικών κοινοτήτων. Οι απευθείας τηλεφωνικές συνδέσεις που λειτουργούν ήδη για να επισημαίνονται τα μηνύματα με παράνομο ή επιζήμιο περιεχόμενο θα μπορούσαν να επεκταθούν και σε άλλες κατηγορίες εγκλημάτων. Μέτρα συστηνόμενα από τους ίδιους του επαγγελματίες και ένα πολυθεματικό μνημόνιο συμφωνίας θα μπορούσαν να συγκεντρώσουν το μεγαλύτερο δυνατό αριθμό ενδιαφερομένων και να διαδραματίσουν πολλαπλό ρόλο στην πρόληψη του εγκλήματος πληροφορικής και την καταπολέμηση αυτού του φαινομένου,, καθώς και στην ενίσχυση της ευαισθητοποίησης και της εμπιστοσύνης του κοινού·

---

[71] Όταν οι ποινικές έρευνες απαιτούν τη συνδρομή των αρχών σε άλλες χώρες, πολλά νομικά συστήματα θέτουν ως προϋπόθεση για ορισμένα είδη αμοιβαίας νομικής συνδρομής και για την έκδοση ότι το αδίκημα πρέπει να είναι αξιόποινο και στις δυο χώρες.

- πρέπει να αντληθεί το μέγιστο δυνατό όφελος από τα επιτεύγματα και τις δυνατότητες της έρευνας και ανάπτυξης. Η στρατηγική που θα ακολουθηθεί θα πρέπει να επιδιώκει να συνταυτίσει την ανάπτυξη προσιτής και αποτελεσματικής ασφάλειας και άλλων τεχνολογιών οικοδόμησης εμπιστοσύνης με τις δράσεις που αναλαμβάνονται σε κοινοτικό επίπεδο.

Εντούτοις, κάθε μέτρο που θεσπίζεται στο μέλλον από την Ευρωπαϊκή Ένωση θα πρέπει να λαμβάνει υπόψη την ανάγκη να οδηγηθούν σταδιακά οι υποψήφιες χώρες στο να συμμετέχουν στην κοινοτική και διεθνή συνεργασία και να αποφευχθεί το ενδεχόμενο να καταστούν καταφύγια του εγκλήματος πληροφορικής. Θα πρέπει να εξεταστεί η συμμετοχή των αντιπροσώπων αυτών των χώρων σε ορισμένες ή στο σύνολο των σχετικών συνεδριάσεων της Ευρωπαϊκής Ένωσης.

Οι προτάσεις της Επιτροπής μπορούν να διαιρεθούν στις ακόλουθες κατηγορίες.

7.1. Νομοθετικές προτάσεις

Η Επιτροπή θα υποβάλει νομοθετικές προτάσεις δυνάμει του τίτλου VI της συνθήκης για την Ευρωπαϊκή Ένωση:

- Για την προσέγγιση των νομοθεσιών των κρατών μελών στον τομέα των εγκλημάτων που αφορούν την παιδική πορνογραφία. Αυτή η πρωτοβουλία θα αποτελέσει μέρος ενός συνόλου προτάσεων που περιλαμβάνουν εξίσου ευρύτερα θέματα που έχουν σχέση με τη σεξουαλική εκμετάλλευση των παιδιών και την εμπορία ανθρώπων, όπως αυτό ανακοινώνεται στην ανακοίνωση της Επιτροπής για την εμπορία ανθρώπων του Δεκεμβρίου 1998. Αυτή η πρόταση θα είναι απολύτως σύμφωνη με τις προσπάθειες που καταβάλλονται από το Ευρωπαϊκό Κοινοβούλιο για να μετατρέψουν την αυστριακή πρωτοβουλία με σκοπό τη θέσπιση απόφασης του Συμβουλίου σχετικά με την παιδική πορνογραφία σε απόφαση πλαίσιο που αξιώνει την προσέγγιση των νομοθεσιών. Αυτό είναι επίσης συνεκτικό με τα συμπεράσματα του Τάμπερε και τη στρατηγική καταπολέμησης του οργανωμένου εγκλήματος που καθορίστηκε από την Ευρωπαϊκή Ένωση για τη νέα χιλιετία. Αυτή η πρωτοβουλία αποτελεί ήδη μέρος του πίνακα αποτελεσμάτων για τη δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης.

- Για την περαιτέρω προσέγγιση των συστημάτων ποινικού δικαίου στον τομέα του εγκλήματος υψηλής τεχνολογίας. Αυτό θα συμπεριλάβει τα εγκλήματα που αφορούν την πειρατεία και τις επιθέσεις μέσω άρνησης υπηρεσίας. Η Επιτροπή θα εξετάσει επίσης τις δυνατότητες καταπολέμησης του ρατσισμού και της ξενοφοβίας στο Διαδίκτυο προκειμένου να υποβάλει, βάσει του τίτλου VI της ΣΕΕ, απόφαση-πλαίσιο που να καλύπτει τις on-line και off-line δραστηριότητες ρατσισμού και ξενοφοβίας. Τέλος, θα εξετασθεί εξίσου το πρόβλημα των παράνομων ναρκωτικών στο Διαδίκτυο·

- Για την εφαρμογή της αρχής της αμοιβαίας αναγνώρισης των προδικαστικών διατάξεων που έχουν σχέση με έρευνες στον τομέα του εγκλήματος στον κυβερνοχώρο και για τη διευκόλυνση των ποινικών ερευνών που αφορούν εγκλήματα πληροφορικής που ενδιαφέρουν περισσότερο του ενός κράτη μέλη, παρέχοντας κατάλληλες εγγυήσεις τήρησης των θεμελιωδών δικαιωμάτων. Αυτή η πρόταση συμβιβάζεται με τις μεγάλες κατευθυντήριες του προγράμματος μέτρων για την αμοιβαία αναγνώριση, η οποία αναφέρει την ανάγκη να εξεταστούν προτάσεις σχετικά με την παροχή και δέσμευση αποδείξεων.

Η Επιτροπή θα εξετάσει το κατά πόσον υπάρχει λόγος να αναληφθεί πρωτοβουλία, ιδιαίτερα νομοθετικού χαρακτήρα, όσον αφορά το θέμα της διατήρησης δεδομένων κίνησης, με βάση, μεταξύ άλλων διαβουλεύσεων, το αποτέλεσμα των εργασιών που θα διεξαχθούν στο συγκεκριμένο τομέα από το μελλοντικό φόρουμ της ΕΕ.

7.2. Μη νομοθετικές προτάσεις

Προβλέπονται μέτρα σε ορισμένους τομείς:

- Η Επιτροπή πρόκειται να δημιουργήσει και να διευθύνει ένα φόρουμ που θα συγκεντρώνει τις αρχές εφαρμογής του νόμου, τους φορείς παροχής υπηρεσιών, τους φορείς δικτύου, τις ενώσεις καταναλωτών και τις αρχές που είναι επιφορτισμένες με την προστασία των δεδομένων, προκειμένου να εντατικοποιήσει τη συνεργασία σε κοινοτικό επίπεδο ευαισθητοποιώντας το κοινό για τους κινδύνους που αντιπροσωπεύει η εγκληματικότητα στο Διαδίκτυο, να προωθήσει τις βέλτιστες πρακτικές στον τομέα της ηλεκτρονικής ασφάλειας, να αναπτύξει αποτελεσματικές διαδικασίες και μέσα για την καταπολέμηση των εγκλημάτων πληροφορικής, καθώς και να παρακινήσει την περαιτέρω ανάπτυξη μηχανισμών έγκαιρης προειδοποίησης και διαχείρισης κρίσεων. Θα πρόκειται για την κοινοτική εκδοχή παρομοίων φόρουμ που λειτουργούν με επιτυχία σε ορισμένα κράτη μέλη. Εκεί όπου δεν υπάρχουν τέτοια φόρουμ η Επιτροπή θα παρακινήσει τα κράτη μέλη να τα δημιουργήσουν. Η κοινοτική διάρθρωση θα ενθαρρύνει και θα διευκολύνει τη συνεργασία μεταξύ αυτών των διαφόρων φόρουμ.

- Η Επιτροπή θα συνεχίσει να προωθεί την ασφάλεια και την εμπιστοσύνη στο πλαίσιο της πρωτοβουλίας *e*Europe, του προγράμματος δράσης για το Διαδίκτυο, του προγράμματος ΤΚΠ και του προσεχούς προγράμματος-πλαισίου έρευνας και τεχνολογικής ανάπτυξης. Αυτό θα περιλαμβάνει την προώθηση της διαθεσιμότητας προϊόντων και υπηρεσιών με επαρκές επίπεδο ασφάλειας και την ενθάρρυνση πιο απελευθερωμένης χρήσης της ισχυρής κρυπτογράφησης μέσω διαλόγου μεταξύ των ενδιαφερομένων μερών.

- Η Επιτροπή θα προωθήσει περαιτέρω σχέδια στο πλαίσιο υφιστάμενων προγραμμάτων για να υποστηρίξει την κατάρτιση του προσωπικού των αρχών δίωξης στα θέματα που αφορούν το έγκλημα υψηλής τεχνολογίας και την έρευνα στον τομέα του εγκλήματος πληροφορικής.

- Η Επιτροπή προτίθεται να χρηματοδοτήσει μέτρα που προορίζονται να βελτιώσουν το περιεχόμενο και τη χρηστικότητα της βάσης δεδομένων των εθνικών νομοθεσιών των κρατών μελών που προβλέπονται από την μελέτη COMCRIME· θα ξεκινήσει εξάλλου μελέτη για να αποκτήσει καλύτερη εποπτεία του χαρακτήρα και του εύρους του εγκλήματος πληροφορικής στα κράτη μέλη.

7.3. Ενέργειες που διεξάγονται στο πλαίσιο άλλων διεθνών φορέων

Η Επιτροπή θα συνεχίσει να διαδραματίζει πλήρως τον ρόλο της φροντίζοντας ώστε τα κράτη μέλη να συντονίζουν τη δράση τους σε άλλους διεθνείς οργανισμούς στους οποίους εξετάζεται το θέμα του εγκλήματος στον κυβερνοχώρο, όπως το Συμβούλιο της Ευρώπης και οι χώρες του G8. Οι πρωτοβουλίες που θα αναλάβει η Επιτροπή στο επίπεδο της Ευρωπαϊκής Ένωσης θα λαμβάνουν δεόντως υπόψη τις προόδους που πραγματοποιούνται στο πλαίσιο άλλων διεθνών φορέων, ενώ θα επιδιώκεται η προσέγγιση στο εσωτερικό της Ευρωπαϊκής Ένωσης.

* * * * *

ΔΗΜΟΣΙΟΝΟΜΙΚΟ ΔΕΛΤΙΟ

1. ΤΙΤΛΟΣ ΤΗΣ ΕΝΕΡΓΕΙΑΣ

Για μια ασφαλέστερη Κοινωνία της Πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής.

2. ΣΧΕΤΙΚΟ ΚΟΝΔΥΛΙΟ ΤΟΥ ΠΡΟΫΠΟΛΟΓΙΣΜΟΥ

B5 302
B5 820
B6 1110, B6 2111, B6 1210

3. ΝΟΜΙΚΗ ΒΑΣΗ

Άρθρα 95, 154 και 155 της Συνθήκης Κ, και άρθρα 29 και 34 της Συνθήκης ΕΕ.

4. ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΕΝΕΡΓΕΙΑΣ

4.1. Γενικοί στόχοι

Η Επιτροπή θα δημιουργήσει και θα διευθύνει ένα φόρουμ της ΕΕ στο οποίο θα συγκεντρώνει τις αστυνομικές και δικαστικές αρχές, τους παρόχους υπηρεσιών Διαδικτύου, τις επιχειρήσεις τηλεπικοινωνιών, τους οργανισμούς πολιτικών ελευθεριών, τους αντιπροσώπους των καταναλωτών, τις αρχές που είναι επιφορτισμένες με την προστασία των δεδομένων και άλλα ενδιαφερόμενα μέρη, με σκοπό να βελτιώσει την αμοιβαία κατανόηση και συνεργασία στο επίπεδο της Ευρωπαϊκής Ένωσης. Αυτό το φόρουμ θα προσπαθήσει να ευαισθητοποιήσει το κοινό για τους κινδύνους εγκληματικότητας στο Διαδίκτυο, να προωθήσει τις βέλτιστες πρακτικές στον τομέα της ασφάλειας, να προσδιορίσει αποτελεσματικά μέσα και διαδικασίες για την καταπολέμηση των εγκλημάτων πληροφορικής και να ενθαρρύνει την περαιτέρω ανάπτυξη μηχανισμών έγκαιρης προειδοποίησης και διαχείρισης κρίσεων. Τα σχετικά έγγραφα θα δημοσιεύονται σε διεύθυνση στο Διαδίκτυο.

4.2. Χρονική διάρκεια της ενέργειας και προβλεπόμενες ρυθμίσεις για την ανανέωσή της

2001 – 2002. Η αξιολόγηση της συνέχισης του φόρουμ θα γίνει, το 2002.

5. ΚΑΤΑΤΑΞΗ ΤΩΝ ΔΑΠΑΝΩΝ Η ΣΟΔΩΝ

5.1. Μη υποχρεωτικές δαπάνες

5.2. Διαχωριζόμενες πιστώσεις

6. ΕΙΔΟΣ ΔΑΠΑΝΩΝ Η ΕΣΟΔΩΝ

Συνεδριάσεις: επιστροφή οδοιπορικών για τους εμπειρογνώμονες			
B5 302A	2001		27.000 ευρώ
B5 302A	2002		40.500 ευρώ
Λειτουργία του φόρουμ, διατήρηση διεύθυνσης στο Διαδίκτυο			
B6 1110	2001	JRC Αποστολές	10.000 ευρώ
B6 2111	2001	JRC Ειδικές πιστώσεις (διάφορα)	15.000 ευρώ
B6 1210	2001	JRC Γενικά έξοδα	50.000 ευρώ
B6 1110	2002	JRC Αποστολές	10.300 ευρώ
B6 2111	2002	JRC Ειδικές πιστώσεις (διάφορα)	15.450 ευρώ
B6 1210	2002	JRC Γενικά έξοδα	51.500 ευρώ
Μελέτες ειδικών θεμάτων			
B6 2111	2001	JRC Ειδικές πιστώσεις (μελέτες)	25.000 ευρώ
B6 2111	2002	JRC Ειδικές πιστώσεις (μελέτες)	25.750 ευρώ
Σύνολο	2001 + 2002		270.500 ευρώ

7. ΔΗΜΟΣΙΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ

Μέθοδος υπολογισμού του συνολικού κόστους της δράσης (σχέση μεταξύ επιμέρους και συνολικού κόστους) :

Επιστροφή οδοιπορικών στους συμμετέχοντες στις συνεδριάσεις. Υπολογίζεται ότι θα πραγματοποιηθούν 2 συνεδριάσεις, το 2001, και 3 συνεδριάσεις, το 2002. Ανά συνεδρίαση, θα επιστρέφονται τα οδοιπορικά 15 εμπειρογνωμόνων. Το μέσο κόστος επιστροφής ανά άτομο υπολογίζεται σε 900 ευρώ.

Το κόστος, όσον αφορά το προσωπικό και τις ειδικές πιστώσεις, της υποδομής και της διοικητικής και τεχνικής υποστήριξης κατανέμεται ανάλογα με τον αριθμό των μελών του προσωπικού που διατίθεται για τις ενλόγω δραστηριότητες. Ο προϋπολογισμός που προορίζεται για τις μελέτες υπολογίζεται με βάση δύο μελέτες το χρόνο και περίπου μια θέση το μήνα.

8. ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΗΣ ΑΠΑΤΗΣ

Τακτικός έλεγχος. Δεν προβλέπονται άλλα συμπληρωματικά μέτρα για την καταπολέμηση της απάτης.

9. ΣΤΟΙΧΕΙΑ ΑΝΑΛΥΣΗΣ ΚΟΣΤΟΥΣ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑΣ

9.1. Ειδικοί και ποσοτικοί στόχοι· πληθυσμός στον οποίον απευθύνεται η ενέργεια

Ενίσχυση της αμοιβαίας κατανόησης και συνεργασίας στο επίπεδο της ΕΕ μεταξύ των διαφόρων ομάδων ενδιαφέροντος οι οποίες είναι: οι αστυνομικές και δικαστικές αρχές, οι πάροχοι υπηρεσιών Διαδικτύου, οι επιχειρήσεις τηλεπικοινωνιών, οι οργανισμοί πολιτικών ελευθεριών, οι αντιπρόσωποι των καταναλωτών, οι αρχές που είναι επιφορτισμένες με την προστασία των δεδομένων και άλλα ενδιαφερόμενα μέρη.

9.2. Αιτιολόγηση της ενέργειας

Το φόρουμ δημιουργήθηκε με σκοπό την ενίσχυση της αμοιβαίας κατανόησης και συνεργασίας στο επίπεδο της ΕΕ μεταξύ των διαφόρων ομάδων ενδιαφέροντος. Αυτό το φόρουμ θα προσπαθήσει να ευαισθητοποιήσει το κοινό για τους κινδύνους εγκληματικότητας στο Διαδίκτυο, να προωθήσει τις βέλτιστες πρακτικές στον τομέα της ασφάλειας, να προσδιορίσει αποτελεσματικά μέσα και διαδικασίες για την καταπολέμηση των εγκλημάτων πληροφορικής και να ενθαρρύνει την περαιτέρω ανάπτυξη μηχανισμών έγκαιρης προειδοποίησης και διαχείρισης κρίσεων.

9.3. Παρακολούθηση και αξιολόγηση της ενέργειας

Η Επιτροπή θα οργανώσει και θα διευθύνει τις συνεδριάσεις του φόρουμ και θα συμμετέχει στις συζητήσεις του. Η Επιτροπή θα διαχειρίζεται τη σχετική διεύθυνση στο Διαδίκτυο. Η ανάγκη συνέχισης του φόρουμ από το 2003 και πέρα θα αξιολογηθεί, το 2002.

10. ΔΙΟΙΚΗΤΙΚΕΣ ΔΑΠΑΝΕΣ

Οι απαιτήσεις όσον αφορά τους ανθρώπινους πόρους θα καλυφθούν από το υφιστάμενο προσωπικό.

10.1. Επιπτώσεις στο προσωπικό

Είδος θέσης	Προσωπικό που θα διατεθεί για τη διαχείριση της ενέργειας		Πηγή		Διάρκεια
	Θέσεις μόνιμων υπαλλήλων	Θέσεις έκτακτων υπαλλήλων	Υφιστάμενοι πόροι στις ενδιαφερό-μενες ΓΔ	Συμπλη-ρωματικοί πόροι	
Μόνιμοι ή έκτακτοι υπάλληλοι Α Β Γ	 0,05	 1,75 0,15	 1,75 0,15 0,05		Ανά έτος επί 2 έτη
Άλλοι πόροι					
Σύνολο	0,05	1,9	1,95		

10.2 Γενική επίδραση των συμπληρωματικών ανθρώπινων πόρων στον προϋπολογισμό

	Ποσά	Μέθοδος υπολογισμού (2001 - 2002)
Μόνιμοι υπάλληλοι	421 200 ευρώ	2 έτη x 108.000 ευρώ x 1,95 θέσεις