

ΣΥΓΓΡΑΦΕΙΣ	Ραπανάκης Σταμάτης, Γιαννοπούλου Ευγενία
ΠΑΝΕΠΙΣΤΗΜΙΟ	Οικονομικό Πανεπιστήμιο Αθηνών
ΤΜΗΜΑ	Τμήμα Πληροφορικής
E-MAIL	stamrapanakis@hotmail.com , jengiannop83@gmail.com

ΤΙΤΛΟΣ ΕΡΓΑΣΙΑΣ : ΠΕΡΙΟΡΙΣΜΟΙ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΣΤΗ ΣΥΓΧΡΟΝΗ ΟΙΚΟΝΟΜΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

Περίληψη

Αυτό το κείμενο διερευνά σε ποιο βαθμό η χρήση ισχυρής κρυπτογραφίας (strong cryptography) προστατεύει την ιδιωτικότητα (privacy) των συναλλαγών των χρηστών. Εξετάζουμε τα ανώνυμα συστήματα ηλεκτρονικών πληρωμών (anonymous e-cash systems) και ισχυρίζομαστε ότι η χρήση τους είναι κατάλληλη σε ένα πολύ στενό εύρος οικονομικών συναλλαγών. Αναλύουμε το ελληνικό νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων και δίνουμε έμφαση στην αντίστοιχη νομοθεσία στο πεδίο των ηλεκτρονικών επικοινωνιών. Καταλήγουμε στο συμπέρασμα ότι η τεχνολογία δεν αρκεί για να διασφαλιστεί η ιδιωτικότητα των συναλλαγών και ότι η εφαρμογή ενός ευέλικτου νομοθετικού πλαισίου θα παραμένει αναγκαία προϋπόθεση για την παροχή ουσιαστικής προστασίας.

I. Εισαγωγή

Το διαδίκτυο έχει συνδεθεί άρρηκτα με την παροχή online υπηρεσιών και έχει προσελκύσει το επενδυτικό ενδιαφέρον από τα πρώτα στάδια ανάπτυξης του. Οι εφαρμογές του ηλεκτρονικού εμπορίου (e-commerce) περιλαμβάνουν σχεδόν όλους τους τομείς της οικονομικής δραστηριότητας. Οι συναλλαγές πραγματοποιούνται με χρήση μέσων όπως οι πιστωτικές κάρτες, τα ηλεκτρονικά μετρητά (e-cash, digital cash) και οι ηλεκτρονικές επιταγές. Λόγω της εμπορικής εκμετάλλευσης υπάρχει μια αύξηση του ενδιαφέροντος για τα προσωπικά δεδομένα των χρηστών των διαφόρων υπηρεσιών. Οι ιδιοκτήτες δικτυακών τόπων προσπαθούν μέσα από τη συλλογή και επεξεργασία αυτών των δεδομένων να δημιουργήσουν το περίγραμμα της συμπεριφοράς των καταναλωτών. Όμως η δημιουργία καταναλωτικών περιγραμμάτων με αυτόν τον τρόπο συνιστά παραβίαση των βασικών αρχών προστασίας δεδομένων. Έρευνες επιβεβαιώνουν ότι η προσβολή της ιδιωτικότητας (privacy) είναι ένα θέμα που προβληματίζει ιδιαίτερα τους χρήστες του διαδικτύου.

Κάθε άνθρωπος έχει το δικαίωμα να διαχειρίζεται τις προσωπικές του πληροφορίες, και κατ' επέκταση την ψηφιακή του ταυτότητα, με τον τρόπο που αυτός ορίζει. Η κατοχύρωση του δικαιώματος του πληροφοριακού αυτοπροσδιορισμού του ατόμου έχει απασχολήσει ιδιαίτερα την κρυπτογραφική κοινότητα [1]. Αντιμέτωπη με αυτήν την πρόκληση, έχει προτείνει μεγάλο αριθμό ηλεκτρονικών συστημάτων πληρωμών (electronic payment systems) που επιτυγχάνουν την πραγματοποίηση ανώνυμων, μη ανιχνεύσιμων πληρωμών. Αυτά τα συστήματα βασίζονται στην ισχυρή κρυπτογραφία, που σημαίνει ότι τα μηνύματα που μεταδίδονται με αυτά δεν μπορούν να κρυπταναλυθούν σε ένα «λογικό» χρονικό διάστημα, ακόμα και με τη χρήση ειδικού εξοπλισμού (που συνήθως διαθέτουν οι κυβερνήσεις κρατών). Υποστηρίζεται ότι η προστασία των προσωπικών δεδομένων πρέπει να βασίζεται σε μαθηματικά μοντέλα, στην ισχύ της κρυπτογράφησης και όχι στην νομοθεσία που υποτίθεται ότι θα παρέχει δικλείδες ασφαλείας στους πολίτες. Θέτουμε τον ισχυρισμό αυτόν υπό αμφισβήτηση και αναλύουμε τις προοπτικές των ανώνυμων συστημάτων ηλεκτρονικών πληρωμών που βασίζονται στην ισχυρή κρυπτογραφία. Αποδεικνύουμε ότι τα συστήματα αυτά δεν έχουν ουσιαστική χρησιμότητα αν δεν προστατεύονται από ένα ευέλικτο νομοθετικό πλαίσιο.

II. Ανώνυμα Συστήματα Ηλεκτρονικών Συναλλαγών

Τα συστήματα ηλεκτρονικών συναλλαγών (πχ. CAFE, NetCash κα) έχουν συγκεκριμένες απαιτήσεις ασφάλειας, όπως έλεγχο αυθεντικότητας και εξουσιοδότηση, εμπιστευτικότητα, ακεραιότητα και μη αποποίηση ευθύνης [2]. Οι ιδιότητες αυτές είναι επιθυμητές αλλά όχι αρκετές για να διαφυλάξουν την ιδιωτικότητα των χρηστών. Η ανεπάρκεια αυτή είναι εντονότερη εάν λάβει κανείς υπόψη του τις θέσεις πολλών ερευνητών, με κύριο εκφραστή τον David Chaum, που έδωσε ευρύτερο ορισμό στον όρο ιδιωτικότητα και πρότεινε, από το 1985, τα ανώνυμα συστήματα ηλεκτρονικών πληρωμών [3][4]. Σύμφωνα με τον David Chaum ιδιωτικότητα σημαίνει ότι το ιστορικό των αγορών κάποιου δεν θα είναι διαθέσιμο για έλεγχο από τράπεζες και εταιρείες πιστωτικών καρτών και κατ' επέκταση ούτε από το κράτος. Υποστήριξε ότι για να είναι οι πολίτες προστατευμένοι από τον «Μεγάλο Αδελφό»

δεν απαιτείται απλά ιδιωτικότητα στις συναλλαγές τους αλλά ανωνυμία (anonymity). Ωστόσο η ανωνυμία εγείρει νέα ζητήματα που πρέπει να αντιμετωπιστούν και έχει αποτελέσει το επίκεντρο μιας έντονης διαμάχης.

Η ηλεκτρονική ανωνυμία δίνει την δυνατότητα στους χρήστες να προβαίνουν σε διάφορες ενέργειες χωρίς να είναι αναγνωρίσιμοι. Μπορούν έτσι να προστατεύουν τα πολύτιμα δεδομένα τους, αφού αυτά είναι ισχυρά κρυπτογραφημένα και δεν μπορεί να εξακριβωθεί ο κάτοχος τους, αλλά από την άλλη πλευρά τυχών συμμετοχή τους σε παράνομες δραστηριότητες είναι εξαιρετικά δύσκολο να ανιχνευτεί. Η εισαγωγή του ανώνυμου ηλεκτρονικού χρήματος (anonymous e-cash) θα αυξήσει το εύρος των δραστηριοτήτων που διεξάγονται ανώνυμα και μοιραία θα εμφανιστούν και δικτυακές απάτες [5]. Επειδή το ανώνυμο ψηφιακό χρήμα είναι μη ανιχνεύσιμο, εκφράζονται φόβοι ότι ο οι δικτυακές απάτες θα είναι πολύ περισσότερες σε σχέση με τα σημερινά συστήματα ηλεκτρονικών πληρωμών. Αν δεν μπορεί να βρεθεί η προέλευση του χρήματος, τότε συναλλαγές όπως το ξέπλυμα βρώμικου χρήματος θα πραγματοποιούνται εύκολα στο διαδίκτυο. Πέρα από την αύξηση της εγκληματικής δραστηριότητας, η ανωνυμία θα επηρεάσει την συμπεριφορά και του απλού, μέσου χρήστη. Σύμφωνα με τον Justice Scalia στο *McIntyre, v. Ohio Elections Commission*, η ανωνυμία είναι ανέντιμη. Υποστηρίζει ότι ένας νομοταγής χρήστης δεν έχει λόγους να θέλει να παραμένει ανώνυμος και ότι η υπάρχουσα (ασθενής) κρυπτογραφία είναι αρκετή για να καλύψει τις ανάγκες του. Αντίθετα, η ανωνυμία μάλλον θα τον διαφθείρει, αφού θα έχει την δυνατότητα να συμπεριφέρεται ανεύθυνα χωρίς να φοβάται μήπως αποκαλυφθεί η ταυτότητα του [6].

Από την άλλη πλευρά, η ανωνυμία έχει και θετικές πλευρές. Σε πολλές χώρες υπάρχουν περιορισμοί στην πρόσβαση στο διαδίκτυο και καταπατούνται τα ατομικά και πολιτικά δικαιώματα. Η ανωνυμία προωθεί την ελευθερία της έκφρασης και τα ανώνυμα συστήματα ηλεκτρονικών πληρωμών συμβάλλουν προς αυτή την κατεύθυνση. Αν ο κρατικός κατασταλτικός μηχανισμός δεν είναι σε θέση να γνωρίζει ποιες περιοχές του διαδικτύου επισκέπτονται οι πολίτες του και με ποιους συναλλάσσονται, τότε οι δυνατότητες του μειώνονται κατά πολύ. Στις δυτικές κοινωνίες εκφράζονται ανησυχίες ότι οι πολίτες είναι απροστάτευτοι από το κράτος ή και από επιχειρήσεις του ιδιωτικού τομέα. Τα συστήματα ηλεκτρονικών πληρωμών είναι δυνατό να καταγράφουν, με κάθε λεπτομέρεια, τις συναλλαγές των χρηστών σε μεγάλες Βάσεις Δεδομένων. Στοιχεία όπως οι αγοραστικές προτιμήσεις των χρηστών, υπόλοιπα πληρωμών και άλλα θα είναι εκτεθειμένα σε μια σειρά εξωτερικών απειλών. Σε ένα υποθετικό μελλοντικό περιβάλλον, τα ηλεκτρονικά καταχωρημένα προφίλ των χρηστών θα αποτελούν αντικείμενο αγοράς και πώλησης [7].

Η ανωνυμία μπορεί να αποτελέσει την λύση σε έναν κόσμο όπου η ποσότητα των προσωπικών μας δεδομένων αυξάνεται καθημερινά και όπου το κράτος και οι επιχειρήσεις μπορούν να αποκτήσουν πρόσβαση σε αυτά [8]. Τα ηλεκτρονικά μετρητά, για παράδειγμα, θα πρέπει να είναι ανώνυμα. Έτσι, η μεταφορά τους από το ένα πρόσωπο στο άλλο θα γίνεται χωρίς να παραμένουν τα ίχνη των προηγούμενων κατόχων τους και η ροή της συναλλαγής θα παραμένει ανεξιχνίαστη [9].

Στην κρυπτογραφική κοινότητα, όπου υπάρχει παραδοσιακά μια ευαισθησία στα θέματα προστασίας προσωπικών δεδομένων, η τάση είναι υπέρ της ανωνυμίας. Προκειμένου να αντιμετωπίσει τις παραπάνω προκλήσεις, στους κόλπους της έχουν προταθεί συστήματα ηλεκτρονικών πληρωμών που εξασφαλίζουν την ανωνυμία σε όλες τις φάσεις της συναλλαγής (όχι μόνο κατά την πληρωμή αυτή καθ' αυτή αλλά και ότι η συναλλαγή θα παραμένει μη ανιχνεύσιμη (untraceable) μετά το πέρας της). Για παράδειγμα, μια τράπεζα μπορεί να μην γνωρίζει τι προϊόντα αγόρασε ένας πελάτης της (τα πλήρη στοιχεία της πληρωμής), μπορεί όμως να συνάγει κάποια συμπεράσματα από την μείωση του ποσού στο λογαριασμό του, οπότε η συναλλαγή δεν παραμένει μη ανιχνεύσιμη μετά το πέρας της. Στα συστήματα αυτά, ο όρος οικονομική κρυπτογραφία (financial cryptography) που σχετίζεται με την προστασία της οικονομικής δραστηριότητας, ταυτίζεται με τον όρο ισχυρή κρυπτογραφία [10].

III. Η ισχυρή κρυπτογραφία στις οικονομικές συναλλαγές

Η ισχυρή κρυπτογραφία είναι ευρέως διαθέσιμη και με χαμηλό κόστος. Το πρώτο γνωστό σύστημα ήταν το PGP (Pretty Good Privacy), που υλοποιήθηκε από τον Philip Zimmermann και αποτελεί σταθμό στην ιστορία της ισχυρής κρυπτογραφίας [18]. Η έκδοση PGP 1.0 διατέθηκε το 1991 στο κοινό και προστάτευε τα e-mail των χρηστών. Την σκυτάλη έχει πάρει η κοινότητα του ανοιχτού λογισμικού (open software) που προσφέρει συστήματα με ισχυρή κρυπτογραφία δωρεάν. Οι επιχειρήσεις χρησιμοποιούν συστήματα ισχυρής κρυπτογραφίας όχι μόνο στις συναλλαγές τους αλλά και σε άλλες λειτουργίες τους. Ανάλογα με την πολιτική ασφάλειας που ακολουθεί μια εταιρεία, μια διαδικτυακή εφαρμογή που χρησιμοποιεί ισχυρή κρυπτογραφία μπορεί να παρέχει μεγαλύτερο βαθμό ασφάλειας σε σχέση με άλλες που έχουν ασθενή κρυπτογράφηση και είναι περιορισμένες στο εταιρικό της δίκτυο. Ύστερα από κατάλληλη μελέτη και διαμόρφωση της πολιτικής ασφάλειας της εταιρείας, εφαρμογές που βασίζονται στο διαδίκτυο και την ισχυρή κρυπτογραφία αποτελούν καλύτερη εναλλακτική σε σχέση με τα πανάκριβα και πολύπλοκα συστήματα κρυπτογραφίας που προσφέρονταν μέχρι πρότινος.

Η χρήση της κρυπτογραφίας στο πεδίο των οικονομικών δραστηριοτήτων μπορεί να διακριθεί σε τέσσερις περιοχές.

Περιορισμοί της Κρυπτογραφίας στη σύγχρονη Οικονομική Δραστηριότητα

Η πρώτη περιοχή αντιπροσωπεύει το σύνολο των συναλλαγών οι οποίες χρησιμοποιούν ισχυρή κρυπτογραφία. Παράδειγμα αποτελούν τα ανώνυμα συστήματα ηλεκτρονικών πληρωμών. Σε αυτού του είδους τις συναλλαγές η κρυπτογραφία παρέχει:

- α) Ανωνυμία στο χρήστη, δηλαδή κανένα τρίτο μέρος δεν μπορεί να μάθει τα στοιχεία του αλλά ούτε και το εάν έγινε κάποια συναλλαγή.
- β) Ολοκληρωμένη ασφάλεια, αφού ακόμα και εάν υποκλέπτονταν οι κρυπτογραφημένες πληροφορίες (παραβιαζόταν η ανωνυμία) τα δεδομένα της συναλλαγής θα ήταν αδύνατο να κρυπταναλυθούν.

Καθώς μετακινούμαστε στη δεύτερη περιοχή, απομακρυνόμαστε από τον πυρήνα των συναλλαγών που προστατεύουν πλήρως την ιδιωτικότητα κατά David Chaum. Στις συναλλαγές αυτές η (ασθενής) κρυπτογραφία που χρησιμοποιείται δεν εξασφαλίζει την ανωνυμία. Ένα παράδειγμα συναλλαγής που ανήκει σε αυτήν την κατηγορία είναι η χρήση μιας πιστωτικής κάρτας μέσω του Internet. Σε αυτήν την περίπτωση, ο αριθμός της πιστωτικής κάρτας είναι κατάλληλα κρυπτογραφημένος ώστε να παρέχει επαρκή ασφάλεια από το ενδεχόμενο απάτης. Όμως η τράπεζα που μεσολάβησε για να χρεωθεί η κάρτα μας γνωρίζει τα στοιχεία μας και ίσως πολλοί άλλοι που μπορεί να μην σχετίζονται με την συναλλαγή. Αν και είμαστε ασφαλείς απέναντι σε τρίτους που μπορεί να προσπαθήσουν να κλέψουν τον αριθμό της πιστωτικής μας κάρτας, δεν διασφαλίζεται η ιδιωτικότητα των προσωπικών μας δεδομένων.

Η επόμενη περιοχή χαρακτηρίζεται από την απουσία κρυπτογραφίας και από το μεγάλο πλήθος των συναλλαγών. Σε αυτήν περιλαμβάνονται μη ηλεκτρονικές συναλλαγές, στις οποίες είναι φανερά τα στοιχεία του αγοραστή, τα μέσα της συναλλαγής (όπως αριθμοί πιστωτικών καρτών, επιταγές), το ποσό και γενικά όλα τα στοιχεία αυτής. Ένα σημαντικό χαρακτηριστικό αυτής της περιοχής είναι πως παρότι δεν χρησιμοποιούνται κρυπτογραφικές μέθοδοι, υπονοείται η εχεμύθεια των προσώπων που εμπλέκονται σε αυτές. Για παράδειγμα, ορισμένοι χρήστες αποκαλύπτουν τον κωδικό της πιστωτικής τους κάρτας από το τηλέφωνο σε μια υπάλληλο, για να αγοράσουν εισιτήρια κινηματογράφου, θεωρώντας ότι αυτή δεν πρόκειται να το σημειώσει και να προβεί μετέπειτα σε αγορές. Υποθέτουμε ότι οι υπάλληλοι μιας τράπεζας που διαχειρίζονται τα στοιχεία μιας συναλλαγής δεν πρόκειται να τα δημοσιοποιήσουν.

Η τέταρτη περιοχή χαρακτηρίζεται από πλήρη απουσία κρυπτογραφίας και διαφοροποιείται από την τρίτη στο ότι τα στοιχεία της συναλλαγής εκτίθενται δημόσια. Τα εμπλεκόμενα μέρη προστατεύονται μόνο από τη νομοθεσία. Παραδείγματα τέτοιων συναλλαγών είναι οι αγοραπωλησίες ακινήτων, όπου ο αγοραστής μπορεί να βρει (βάζοντας έναν δικηγόρο να ψάξει στο υποθηκοφυλακείο) εάν το ακίνητο που θέλει να αγοράσει είναι υποθήκη ή ποιος είναι ο πραγματικός ιδιοκτήτης του. Τα στοιχεία αυτών των συναλλαγών είναι εύκολα προσβάσιμα σε κάθε ενδιαφερόμενο [10].

Το μεγαλύτερο ποσοστό των καθημερινών συναλλαγών είναι μη ασφαλείς και η ιδιωτικότητα των εμπλεκόμενων μερών είναι είτε είναι εκτεθειμένη είτε απλά δεν υφίσταται. Στις δυο τελευταίες περιοχές συναλλαγών η διαφύλαξη της ιδιωτικότητας δεν έχει νόημα για τους περισσότερους χρήστες. Σχετική προσπάθεια θα έκανε τις συναλλαγές αυτές πιο πολύπλοκες και θα αύξανε το κόστος τους. Αντίθετα, στα ηλεκτρονικά συστήματα πληρωμών η κρυπτογραφία δεν πρέπει απλώς να θεωρείται ανάγκη, αλλά απαίτηση.

IV. Ανωνυμία και προβλήματα χρηστών

Δεδομένης της ανησυχίας για εκμετάλλευση των προσωπικών δεδομένων των χρηστών και της τάσης για επικράτηση της ανωνυμίας σε συστήματα ηλεκτρονικών συναλλαγών, θα εξετάσουμε ποιες είναι οι προοπτικές των ανώνυμων συστημάτων ηλεκτρονικών πληρωμών. Επίσης θα κάνουμε την παραδοχή ότι η ισχυρή κρυπτογραφία δεν περιορίζεται από το υφιστάμενο νομικό πλαίσιο, όπως συμβαίνει σε ορισμένες χώρες.

1) *Οι συναλλαγές δανειοληψίας προβλέπεται να είναι εξαιρετικά δύσκολο έως αδύνατο να πραγματοποιηθούν με ανώνυμους δανειολήπτες.* Οι τράπεζες δεν θα έχουν στοιχεία για την αξιοπιστία των πελατών τους (credit history). Τα στοιχεία αυτά είναι απαραίτητα για να εκτιμηθεί το επιχειρηματικό ρίσκο και να διαμορφωθεί σε ένα βαθμό και το επιτόκιο του δανείου. Το αποτέλεσμα της άγνοιας τους θα ήταν η αύξηση των επιτοκίων καθώς οι τράπεζες θα ήθελαν να καλύψουν το ρίσκο που θα προέκυπτε από ανεύθυνους δανειολήπτες, σε βάρος όμως και τον υπεύθυνων δανειοληπτών. Προφανώς, οι περισσότεροι άνθρωποι δεν θα προτιμούσαν να έχουν υψηλότερο επιτόκιο με κέρδος μια ανώνυμη δανειοληψία.

2) *Η διαχείριση των κλειδιών ώστε να διατηρηθεί η ανωνυμία των χρηστών αποτελεί ασθενές σημείο.* Στον κόσμο της ισχυρής κρυπτογραφίας, η απώλεια ενός κλειδιού είναι καταστροφική από τον ορισμό της: ισχυρή κρυπτογραφία σημαίνει πως κανείς δεν μπορεί να «σπάσει» τον κώδικα του μηνύματος (μέσα σε ένα λογικό χρονικό διάστημα). Αν τα ηλεκτρονικά μετρητά είναι κρυπτογραφημένα, τότε η απώλεια του κλειδιού που τα κρυπταναλύει συνεπάγεται άμεση απώλεια των χρημάτων [10]. Η διαχείριση ενός κλειδιού αποτελείται από τα στάδια της επιλογής ενός καλού κλειδιού, της αποθήκευσής του, της ασφαλούς προστασίας του, της ανανέωσής

του και της υποχρεωτικής διαφοροποίησής του από άλλα κλειδιά που πιθανόν να έχει και να χρησιμοποιεί ο κάτοχός του [11]. Όλα αυτά δυσκολεύουν και κουράζουν ακόμα και τους χρήστες που είναι εξοικειωμένοι με την τεχνολογία. Αυτό δημιουργεί προβλήματα, πόσο μάλλον αν αναλογιστούμε ότι ο περισσότερος κόσμος δυσκολεύεται να θυμάται ένα απλό τετραψήφιο PIN. Συμπεραίνουμε πως η σωστή διαδικασία διαχείρισης ενός κλειδιού, η οποία δεν θα έθετε σε κίνδυνο την ανωνυμία του, δεν είναι φιλική προς το χρήστη. Ακόμα και αν ο χρήστης επιλέξει να αναθέσει τη διαχείριση των κλειδιών του σε κάποιον ειδικό (πχ τράπεζα, εταιρεία), θα πρέπει να λάβει υπόψη του το γεγονός ότι ο ειδικός μπορεί να είναι κακόβουλος ή να του συμβεί κάτι και να μην είναι διαθέσιμος την κατάλληλη στιγμή.

3) Η εξάπλωση των κρυπτογραφικών μηχανισμών θα αντιμετωπίσει προβλήματα αποδοχής από το καταναλωτικό κοινό. Τα συστήματα ηλεκτρονικών συναλλαγών που χρησιμοποιούνται, παρά τα προβλήματα που κατά καιρούς αντιμετωπίζουν, δεν δείχνουν ότι μπορούν να αντικατασταθούν στο άμεσο μέλλον. Οι χρήστες τα εμπιστεύονται και δεν είναι διατεθειμένοι να τα εγκαταλείψουν για χάρη της ανωνυμίας. Προκειμένου να κατακτήσει ένα σύστημα ηλεκτρονικών πληρωμών την εμπιστοσύνη του αγοραστικού κοινού, απαιτείται μεγάλο χρονικό διάστημα. Αν αναλογιστούμε τη δυσκολία αποδοχής των ATM των τραπεζών, οδηγούμαστε στη διαπίστωση ότι οι ισχυροί κρυπτογραφικοί μηχανισμοί μπορεί να καθυστερήσουν πολύ μέχρι να εδραιωθούν.

V. Προστασία των προσωπικών δεδομένων και ελληνική νομοθεσία

Η προστασία των προσωπικών δεδομένων αποτελεί ένα από τα πιο θεμελιώδη ανθρώπινα δικαιώματα. Η νομοθεσία είναι ένα αποτελεσματικό μέσο διασφάλισης του δικαιώματος αυτού. Το ελληνικό νομοθετικό πλαίσιο προστασίας προσωπικών δεδομένων συγκροτείται κυρίως από την οικεία συνταγματική ρύθμιση και το νόμο 2472/97 [12]. Υπάρχουν ωστόσο και ρυθμίσεις που είτε άπτονται της προστασίας προσωπικών δεδομένων είτε παραπέμπουν στον παραπάνω νόμο για την παροχή εγγυήσεων στην περίπτωση της προστασίας προσωπικών δεδομένων (όπως ο Ν. 2928/01 που αφορά την καταπολέμηση του οργανωμένου εγκλήματος).

Κατά την τελευταία αναθεώρηση του Συντάγματος (2001) περιλήφθηκε το άρθρο 9Α που ορίζει ότι ο “καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει. Η διασφάλιση της προστασίας των προσωπικών δεδομένων ανατίθεται από τον αναθεωρητικό νομοθέτη σε ανεξάρτητη αρχή που συγκροτείται και λειτουργεί όπως ο νόμος ορίζει”.

Μέσα από την συνταγματική κατοχύρωση η προστασία των προσωπικών δεδομένων ανάγεται σε αυτοτελές δικαίωμα. Φορείς του δικαιώματος αυτού δεν είναι μόνο οι έλληνες πολίτες αλλά κάθε άνθρωπος. Η προστατευτική εμβέλεια του άρθρου καλύπτει κάθε δεδομένο, δηλαδή κάθε πληροφορία που αφορά ένα πρόσωπο και όχι μόνο τα απόρρητα [13]. Επίσης εξασφαλίζει το άτομο όχι μόνο έναντι της κρατικής εξουσίας αλλά και έναντι των ιδιωτών. Όσον αφορά την εγγύηση της προστασίας των προσωπικών δεδομένων ορίζεται από το Σύνταγμα η θεσμοθέτηση ανεξάρτητης αρχής με αποστολή την διασφάλιση του δικαιώματος.

Ως βασική προϋπόθεση για τη νομιμότητα επεξεργασίας προσωπικών δεδομένων ορίζεται η συγκατάθεση του υποκειμένου των δεδομένων [14]. Η συγκατάθεση αυτή θα πρέπει να είναι σαφής και να παρέχεται μετά από εκτενή πληροφόρηση [15]. Παράλληλα ο νόμος ορίζει και περιπτώσεις που δεν υπάρχει ή δεν μπορεί να υπάρξει συγκατάθεση του ατόμου, όπως η εκτέλεση σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή η εκτέλεση έργου δημοσίου συμφέροντος. Η ρύθμιση αυτή χαρακτηρίζεται από γενικότητα και ασάφεια με αποτέλεσμα συχνά να ερμηνεύεται υπέρ των ιδιαίτερων συμφερόντων της επεξεργασίας. Η ερμηνεία της διέπεται από δύο περιορισμούς: την ειδική αξιολόγηση των προβλεπόμενων ως εξαιρέσεων καθώς και τον σκοπό του νόμου που συνίσταται στην διασφάλιση των θεμελιωδών δικαιωμάτων και ελευθεριών του ανθρώπου.

Ο νόμος διατυπώνει ρητά την υποχρέωση καταστροφής των δεδομένων μετά την πραγματοποίηση του σκοπού συλλογής και επεξεργασίας τους, με εξαίρεση ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς [16]. Οι ποσοτικές αλλαγές στην επεξεργασία δεδομένων, η αύξουσα εμπορευματοποίηση τους αλλά και οι ποιοτικές αλλαγές που χαρακτηρίζουν τη φύση των δεδομένων που υπόκεινται σε επεξεργασία, μας οδηγούν να προσανατολιστούμε σε μία ακόμη στενότερη προσέγγιση της αρχής του σκοπού που σημαίνει μεταξύ άλλων τον συνειδητό αποκλεισμό κάθε χρήσης που δεν είναι ρητά επιτρεπτή [15].

Βασική επιλογή του νομοθέτη είναι να παρέχει τη δυνατότητα στα φυσικά πρόσωπα να γνωρίζουν και να συν-προσδιορίζουν ποιες πληροφορίες που τους αφορούν μπορούν να αποτελέσουν αντικείμενο επεξεργασίας. Τα δικαιώματα που κατοχυρώνει ο νόμος είναι το δικαίωμα της ενημέρωσης, πρόσβασης, διόρθωσης και διαγραφής, αντίρρησης καθώς και το δικαίωμα προσωρινής δικαστικής προστασίας. Αν και με τις ρυθμίσεις αυτές επιδιώκεται η «θωράκιση» του υποκειμένου των δεδομένων, ο μεμονωμένος ιδιώτης δεν είναι σε θέση να ελέγξει την πληροφοριακή δομή και συμπεριφορά της διοίκησης. Το χάσμα γνώσεων και δυνατοτήτων που χωρίζει το μέσο πολίτη από αυτούς που επεξεργάζονται προσωπικές πληροφορίες διευρύνεται διαρκώς. Ένα επιπλέον βασικό μειονέκτημα είναι ότι δεν είναι δυνατή η συναγωγή ασφαλών συμπερασμάτων για την νομιμότητα και τις τάσεις των διαδικασιών επεξεργασίας [17].

VI. Ηλεκτρονικές επικοινωνίες και διεθνής νομολογία

Το διαδίκτυο θέτει νέα ζητήματα ως προς την επεξεργασία και την προστασία των προσωπικών δεδομένων. Παρά τις αντιλήψεις που φαίνεται να επικρατούσαν τα πρώτα χρόνια της έκρηξης του διαδικτύου, πρέπει να επισημάνουμε ότι αυτό δεν αναπτύσσεται σε ένα «νομικό κενό». Η διαμόρφωση της πολιτικής που αφορά το Διαδίκτυο και τα επιμέρους άλλα μείζονα ζητήματα που αυτό θέτει πραγματοποιείται βάσει σαφώς καθορισμένων αρχών και αξιών.

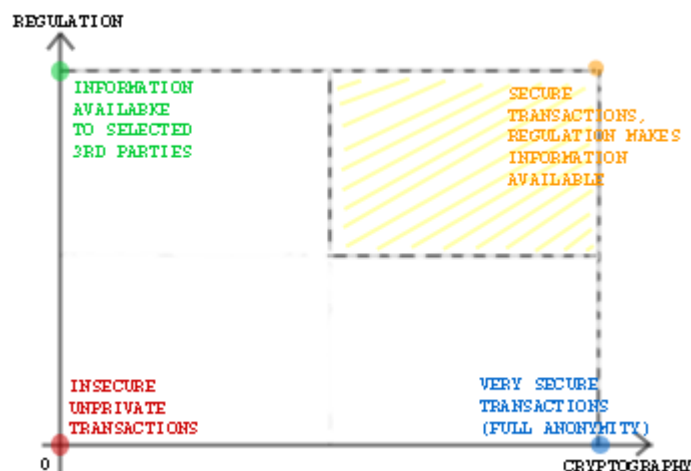
Η Οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου αναφέρεται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η ρύθμιση του άρθρου 5 ενισχύει τις αρχές της εμπιστευτικότητας και της ανωνυμίας, δεσμεύοντας τα κράτη μέλη να επεκτείνουν την προστασία του απορρήτου και στα «συναφή δεδομένα κίνησης» (όπως δρομολόγηση, διάρκεια κίνησης, τερματικός εξοπλισμός χρήστη κα).

Στο προοίμιο της Οδηγίας (20) επισημαίνεται ο κίνδυνος παραβίασης της ασφάλειας του Διαδικτύου και του δικτύου της αναλογικής κινητής τηλεφωνίας. Ο πάροχος υπηρεσιών έχει την υποχρέωση να εξασφαλίζει ένα αποδεκτό επίπεδο ασφάλειας του δικτύου του. Κρίσιμη είναι η επισήμανση ότι η απαγόρευση της αποθήκευσης των επικοινωνιών χωρίς τη συγκατάθεση των χρηστών, δεν αποκλείει τυχόν αυτόματη, ενδιάμεση και παροδική αποθήκευση των πληροφοριών εφόσον αυτή γίνεται με μοναδικό σκοπό την πραγματοποίηση της μετάδοσης στο ηλεκτρονικό δίκτυο επικοινωνιών και υπό την προϋπόθεση ότι οι πληροφορίες δεν αποθηκεύονται για διάστημα μεγαλύτερο απ' όσο απαιτείται για τη μετάδοση και για σκοπούς διαχείρισης της κίνησης. Είναι αυτονόητο ότι κατά της περιόδου αποθήκευσης πρέπει να διατηρούνται οι εγγυήσεις του απορρήτου.

Το νομοθετικό πλαίσιο της προστασίας του απορρήτου των επικοινωνιών στην Ελλάδα και γενικότερα στην Ευρωπαϊκή Ένωση είναι πιο ισχυρό από το αντίστοιχο των ΗΠΑ. Χαρακτηριστικό παράδειγμα αποτελεί η διαφορετική αντίληψη αναφορικά με το λογισμικό κρυπτογράφησης. Μέχρι πριν από λίγα χρόνια, οι αμερικανικές εταιρίες αντιμετώπιζαν περιορισμούς στην εξαγωγή προγραμμάτων κρυπτογραφίας με ιδιωτικό κλειδί μεγαλύτερο από 56bits καθώς απαιτούσε ειδική άδεια από το Αμερικανικό Υπουργείο Εξωτερικών. Σήμερα ισχύει αντίστοιχη νομοθεσία, αλλά για προϊόντα με ιδιωτικό κλειδί μεγαλύτερο από 128 bits. Παρατηρητές υποστηρίζουν ότι αυτό συμβαίνει απλά και μόνο επειδή η κυβέρνηση των ΗΠΑ διαθέτει σήμερα την τεχνολογία να κρυπτανάλυει μηνύματα αυτής της κωδικοποίησης. Αντίθετα, στην Ευρωπαϊκή Ένωση έχουν αρθεί αντίστοιχοι περιορισμοί και ο νομοθέτης έχει αναπτύξει δικλίδες ασφαλείας που δεν σχετίζονται με την ισχύ της κωδικοποίησης.

VII. Συμπεράσματα

Οι απόψεις γύρω από την διασφάλιση της ιδιωτικότητας των συναλλαγών μπορούν να παρασταθούν σχήμα 1. Παρατηρούμε στο κάτω αριστερό άκρο την κατηγορία συναλλαγών στις οποίες δεν παρέχεται ασφάλεια ούτε από την ισχυρή κρυπτογραφία ούτε από τη νομοθεσία. Κάτι τέτοιο δεν είναι επιθυμητό σε καμία περίπτωση. Κανένας χρήστης δεν θέλει να συμμετέχει σε συναλλαγές που θα εκθέτουν τα προσωπικά του δεδομένα και όπου θα μπορεί να είναι εύκολα θύμα απάτης. Οι συναλλαγές που περιγράφονται από το πάνω αριστερό άκρο παρέχουν πληροφορίες σε επιλεγμένες ομάδες ατόμων οι οποίες καθορίζονται αποκλειστικά από τη νομοθεσία. Οι χρήστες είναι εξαρτημένοι από την κρατική μονοθεσία, η οποία δεν τους παρέχει προστασία ούτε από την ίδια, ούτε και από τρίτους. Μια τέτοια κατάσταση δεν ευνοεί την ανάπτυξη ηλεκτρονικών συναλλαγών και καταπατά τα βασικά ανθρώπινα δικαιώματα.



Σχήμα 1

Στο κάτω δεξί άκρο περιλαμβάνονται οι συναλλαγές που είναι πολύ ασφαλείς λόγω της ύπαρξης ισχυρής κρυπτογραφίας. Ωστόσο, όπως είδαμε σε προηγούμενη παράγραφο, η ισχυρή κρυπτογραφία και η ανωνυμία που αυτή παρέχει στους χρήστες, σε ένα περιβάλλον που δεν υπόκειται σε κανέναν νομοθετικό έλεγχο, αντιμετωπίζει δυσκολίες αποδοχής στην πράξη. Πέρα από την διστακτικότητα των χρηστών, τα ανώνυμα συστήματα μπορούν να λειτουργήσουν αποτελεσματικά σε ένα περιορισμένο εύρος οικονομικής δραστηριότητας.

Στο σκιαγραφημένο τμήμα του γραφήματος (πάνω και δεξιά), εντοπίζουμε τις συναλλαγές που συνδυάζουν τόσο ισχυρές μεθόδους κρυπτογραφίας όσο και προστατεύονται από νομικά πλαίσια. Πιστεύουμε πως αυτού του είδους οι συναλλαγές είναι καταλληλότερες για να προστατεύσουν τον χρήστη και να πραγματοποιούνται ασφαλέστερες ηλεκτρονικές συναλλαγές. Αυτό που προτείνουμε μπορεί να περιγραφεί με τον όρο *επιλεκτική ανωνυμία*. Πρέπει να λαμβάνουμε υπόψη μας το γεγονός ότι οι χρήστες δεν είναι εξοικειωμένοι με πολύπλοκα συστήματα και πως αναζητούν φιλικές προς αυτούς διαδικασίες.

Καταλήγουμε στο συμπέρασμα ότι ο συνδυασμός

- i) Ισχυρής κρυπτογραφίας
- ii) Εφαρμογής ενός ευέλικτου νομοθετικού πλαισίου
- iii) Υιοθέτησης ενός προσιτού ηλεκτρονικού συστήματος προς τον κάθε απλό χρήστη αποτελεί αναγκαία προϋπόθεση για την παροχή ολοκληρωμένης προστασίας στις σύγχρονες οικονομικές συναλλαγές.

Αναφορές

- [1] Σωκράτης Κάτσικας , Στέφανος Γκρίτζαλης, Δημήτρης Γκρίτζαλης. *Ασφάλεια πληροφοριακών συστημάτων*. Εκδόσεις Νέων Τεχνολογιών 2004
- [2] Laurie Law, Susan Sabett, Jerry Solinas. *How to make a mint: The cryptography of anonymous electronic cash*. National Security Agency, Office of Information Security Research and Technology, Cryptology Division 1996
- [3] David Chaum, *Achieving Electronic Privacy*, Scientific American (August 1992), 96-101.
- [4] David Chaum, *Security without Identification: Transaction Systems to make Big Brother Obsolete*, ACM 28 no. 10 (Oct 1985), 1030-1044.
- [5] David R. Johnson, David G. Post. *Law and Borders: The Rise of Law in Cyberspace*. 48 Stanford L Rev 1367 1996.
- [6] Justice Scalia. *McIntyre, v. Ohio Elections Commission*. 63 U.S.L.W.4279 (US April 18 1995). Scalia, J. dissenting slip. Op. No. 93-986 April 19, 1995).
- [7] Ronald L. Rivest. *Perspectives on Financial Technology*.
- [8] A. Michael Froomkin. *Anonymity and Its Enemies*. 1995
- [9] Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας, Δημήτρης Γκρίτζαλης. *Ασφάλεια δικτύων υπολογιστών*. Εκδόσεις Παπασωτηρίου 2003
- [10] Wikipedia
- [11] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons 1996
- [12] Kaissis, A. *Datenschutz in Griechenland*, Hamburg 1996
- [13] Λαζαράτος Π., *Το δικαίωμα της ακροάσεως στη διοικητική διαδικασία*, Αθήνα 1992
- [14] Μήτρου Λ., *Η Αρχή Προστασίας Προσωπικών Δεδομένων*, Κέντρο Ευρωπαϊκού Συνταγματικού Δικαίου – Forum Σύγχρονη Πολιτεία, Τόμος 1, Εκδόσεις Α. Σάκκουλα, Αθήνα 1999
- [15] Simitis S., *Legal and political context of the protection of personal information and privacy* (Paper 1998)
- [16] Simitis S., *Reviewing Privacy in an Information Society*, University of Pennsylvania Law Review 135 (1987)
- [17] Μήτρου Λ., “Ο θεσμικός έλεγχος της προστασίας προσωπικών πληροφοριών” στο συλλογικό έργο: *Ελληνική Εταιρία Επιστημόνων Πληροφορικής και Υπολογιστών (ΕΠΥ)*, *Ασφάλεια πληροφοριών – Τεχνικά, Νομικά και Κοινωνικά θέματα*, Αθήνα 1996
- [18] P.R.Zimmermann, *The Official PGP User’s Guide*, Boston: MIT Press, 1995