

Τα προσωπικά δεδομένα και οι νέες προκλήσεις¹

Οι τεχνολογικές, οικονομικές και πολιτικές εξελίξεις οδηγούν διεθνώς σε μια κοινωνία χωρίς σύνορα, όπου η αξία και ο όγκος της διακινούμενης πληροφορίας αυξάνεται διαρκώς. Θα επικεντρώσω την ομιλία μου στις προκλήσεις που θέτουν για την προστασία των προσωπικών δεδομένων η ανάπτυξη των νέων τεχνολογιών, η παγκοσμιοποίηση της οικονομίας και η τάση ενίσχυσης της δημόσιας ασφάλειας.

Χρίστος Γεραρής,

Πρόεδρος ΑΠΔΠΧ

ρου και παρέχουν σε κάθε μεμονωμένο χρήστη τη δυνατότητα να δημοσιοποιεί δεδομένα όχι μόνο δικά του αλλά και τρίτων προσώπων. Ακόμη και όταν ο χρήστης διαγράφει τα δεδομένα, αυτά

μπορεί να μη διαγραφούν από το πληροφοριακό σύστημα του παρόχου. Είναι πλέον γνωστό ότι και οι εργοδότες χρησιμοποιούν αυτές τις υπηρεσίες για την αξιολόγηση υποψηφίων. Επίσης, πολύ σημαντική εξέλιξη είναι ότι οι υπηρεσίες αυτές δεν χρησιμοποιούνται μόνο για σκοπούς ιδιωτικούς αλλά και για την ανάπτυξη νέων επιχειρηματικών μοντέλων, εννοώ τις διαδικτυακές επιχειρηματικές κοινότητες που συμπράττουν ευκαιριακά για την επίτευξη συγκεκριμένου επιχειρηματικού σκοπού. Επίσης, και ο δημόσιος τομέας αξιοποιεί αυτές τις υπηρεσίες, ιδίως για την προώθηση της συμμετοχικής δημοκρατίας.

Συμπερασματικά οι νέες τεχνολογίες χρησιμοποιούνται από τον ιδιωτικό τομέα για την ανάπτυξη καινοφανών επιχειρηματικών μοντέλων, από το δημόσιο τομέα για την ανάπτυξη εφαρμογών ηλεκτρονικής διακυβέρνησης και συμμετοχικής δημοκρατίας, από τον καθένα μας για σκοπούς προσωπικούς, που ανάγονται στην ενημέρωση, την κοινωνικοποίηση, την ανάπτυξη της ελευθερίας του λόγου και τη διάχυση νέων επιστημονικών και άλλων ιδεών.

Οι τεχνολογικές αυτές εξελίξεις θέτουν την προστασία των προσωπικών δεδομένων απέναντι σε νέες προκλήσεις. Από το στατικό μοντέλο επεξεργασίας, με τους μεγάλους επεξεργαστές εγκατεστημένους σε υπηρεσίες του δημόσιου τομέα ή σε εταιρείες του ιδιωτικού τομέα, περνάμε σταδιακά στο διάχυτο και δυναμικό μοντέλο επεξεργασίας των προσωπικών δεδομένων. Απαιτείται, συνεπώς, ένα νέο θεσμικό πλαίσιο με την επανεξέταση και προσαρμογή βασικών εννοιών της προστασίας των προσωπικών δεδομένων, ιδίως του «υπευθύνου επεξεργασίας», των εργασιών που συνιστούν «επεξεργασία προσωπικών δεδομένων» και του εφαρμοστέου δικαίου. Στις υποδομές κατανεμημένης υπολογιστικής ισχύος αλλά και στις διαδικτυακές κοινότητες χρηστών αναρωτιέται κανείς ποιος θα πρέπει να θεωρείται υπεύθυνος επεξεργασίας, για την τήρηση των νόμιμων υποχρεώσεων και ποιο δίκαιο θα πρέπει να εφαρμοστεί σε κάθε συγκεκριμένη περίπτωση. Όταν δεν ξέρουμε, για παράδειγμα, πού είναι αποθηκευμένα τα δεδομένα, δύσκολα μπορούμε να προσδιορίσουμε ποιο

1. Ανάπτυξη νέων τεχνολογιών

Διαπιστώνουμε ότι η τεχνολογία παρέχει ολοένα και περισσότερες δυνατότητες:

α) Τα νέα ψηφιακά εργαλεία (όπως οι μηχανές αναζήτησης, η ταυτοποίηση μέσω ραδιοσυχνοτήτων (RFIDs), η βιομετρία, οι υπηρεσίες εικονικής περιήγησης σε δρόμους πόλεων και γεωχωρικού εντοπισμού) δημιουργούν κατά τη χρήση τους ίχνη στο χώρο και το χρόνο χωρίς αυτό να γίνεται άμεσα αντιληπτό. Οι τεχνολογίες αυτές, εφόσον παρέχουν πλεονεκτήματα, είναι προσφιλείς στους χρήστες.

β) Η υπολογιστική ισχύς των πληροφοριακών συστημάτων αυξάνει και σε συνδυασμό με τις τεχνολογίες επικοινωνιών, οδηγεί σε ένα παγκόσμιο περιβάλλον διάχυτου υπολογισμού, όπου η επεξεργασία δεδομένων πραγματοποιείται σε υπολογιστές που βρίσκονται οπουδήποτε στον κόσμο χωρίς ο χρήστης της υπηρεσίας να γνωρίζει τον τόπο αποθήκευσης των δεδομένων. Οι υποδομές κατανεμημένης υπολογιστικής ισχύος μέσω του διαδικτύου προσφέρουν ακριβώς υπηρεσίες υπολογιστικής και αποθηκευτικής ισχύος, είτε πρόκειται για τα λεγόμενα πλέγματα υπολογιστών (grids) που χρησιμοποιούνται κυρίως στις μεγάλες ευρωπαϊκές ερευνητικές υποδομές είτε για το λεγόμενο «υπολογιστικό - σύννεφο» (cloud computing).

γ) Η επικοινωνία και ανταλλαγή δεδομένων μέσω υπηρεσιών κοινωνικής δικτύωσης (όπως το Facebook) καθιστούν ασαφή τα όρια μεταξύ δημόσιου και ιδιωτικού χώ-

1. Χαιρετιστήριο ομιλία με τη συνεργασία της ελέγκτριας της ΑΠΔΠΧ, Ζωής Καρδασιάδου, Δικηγόρου, Δ.Ν. στο 3ο Συνέδριο του Επιστημονικού Συμβουλίου για την Κοινωνία της Πληροφορίας, «Ηλεκτρονική Δημοκρατία 2009», Σεπτέμβριος 2009.

δίκαιο θα εφαρμοστεί. Όταν μια επεξεργασία διενεργείται παράλληλα από περισσότερες οντότητες (νομικά ή φυσικά πρόσωπα) και μάλιστα εγκατεστημένες σε διαφορετικές χώρες, το εφαρμοστέο δίκαιο για την ίδια επεξεργασία αποτελεί ζήτημα υπό διερεύνηση. Όταν οι υπηρεσίες κοινωνικής δικτύωσης προκαθορίζουν τον τρόπο επεξεργασίας των δεδομένων μέσω των επιλογών που παρέχουν στους χρήστες για τη διαχείριση των δεδομένων που αναρτούν, είναι δύσκολο να προσδιοριστεί ο υπεύθυνος επεξεργασίας και τούτο διότι ο νόμος προβλέπει ότι ο υπεύθυνος επεξεργασίας προσδιορίζει τον σκοπό και τον τρόπο, δηλαδή τα μέσα, της επεξεργασίας. Στη συγκεκριμένη περίπτωση ο χρήστης σε σχέση με δεδομένα τρίτων προσδιορίζει το σκοπό της επεξεργασίας, δεν έχει όμως ενδεχομένως εξουσία στα μέσα, στον τρόπο δηλαδή της επεξεργασίας, όταν δεν ελέγχει την πλήρη διαγραφή των δεδομένων ή ποιοι έχουν πρόσβαση σε αυτά. Έτσι αποτελεί, ζητούμενο εάν μόνο ο χρήστης ή και ο πάροχος της υπηρεσίας μπορούν να θεωρηθούν υπεύθυνοι της επεξεργασίας.

Επίσης, πρέπει να δοθεί έμφαση στο σκοπό της επεξεργασίας, υπό την έννοια ότι αυτός πρέπει να δηλώνεται με σαφήνεια εκ των προτέρων και η επεξεργασία των προσωπικών δεδομένων να μην επιτρέπεται για άλλους σκοπούς. Πολλές φορές οι σκοποί δεν είναι εύκολα διακριτοί μεταξύ τους και στο ιαχύνον δίκαιο μιλάμε για δευτερογενείς σκοπούς που μπορεί να είναι συμβατοί ή ασύμβατοι με τον αρχικά δηλούμενο σκοπό με αποτέλεσμα συγκεκριμένη επεξεργασία να επιτρέπεται ή μη. Στο νέο όμως τεχνολογικό περιβάλλον η συμβατότητα αυτή θα πρέπει να εξετάζεται με μεγαλύτερη αυστηρότητα ώστε να είναι σαφή και διαφανή τα όρια της επιτρεπόμενης επεξεργασίας. Για παράδειγμα η στοχευμένη διαφήμιση μέσω των υπηρεσιών κοινωνικής δικτύωσης δεν εμπίπτει στον πρωτογενή σκοπό της υπηρεσίας και δεν μπορεί να επιτρέπεται χωρίς τη συγκατάθεση του χρήστη.

Πέραν των νομοθετικών τροποποιήσεων, τις οποίες βλέπω να πραγματοποιούνται σε ορίζοντα πενταετίας διότι θα πρέπει να συζητηθούν σε ευρωπαϊκό επίπεδο, δηλαδή στο πλαίσιο αναθεώρησης της Οδηγίας 95/46/ΕΚ, θα πρέπει να επικεντρώσουμε την προσοχή μας και στις ίδιες τις τεχνολογίες. Αποτελεί πλέον κοινό τόπο ότι η έλλειψη εμπιστοσύνης στις ηλεκτρονικές υπηρεσίες αποτελεί ανασταλτικό παράγοντα για την επέκταση της εφαρμογής τους. Επιβάλλεται η επιλογή λύσεων που εκθέτουν κατά το λιγότερο δυνατό τρόπο τα προσωπικά δεδομένα των χρηστών. Ο ιδιωτικός τομέας πρέπει να αντιληφθεί ότι η προστασία των προσωπικών δεδομένων δεν αποτελεί εμπόδιο στις συναλλαγές αλλά μέτρο κοινωνικής ευθύνης και ανταγωνιστικό πλεονέκτημα. Ο δημόσιος τομέας πρέπει να ενθαρρύνει την επιλογή τεχνολογικών λύσεων που κατά το δυνατό συνδυάζουν την προστασία των προσωπικών δεδομένων με τις ανάγκες της δημόσιας διοίκησης και όλων των φορέων δημόσιας εξουσίας. Τέτοιες τεχνολογικές λύσεις υπάρχουν

και είναι εφικτές, άλλοτε με πιο συστηματικό σχεδιασμό των υπηρεσιών, άλλοτε με μεγαλύτερο οικονομικό κόστος, το οποίο όμως, όταν δεν είναι δυσανάλογο, παρέχει διέξοδο στην ικανοποίηση αντίρροπων συμφερόντων.

2. Η παγκοσμιοποίηση της οικονομίας

Η παγκοσμιοποιημένη οικονομία αυξάνει την ανάγκη διακίνησης προσωπικών δεδομένων είτε μεταξύ ομίλων εταιρειών είτε μεταξύ συνεργαζόμενων εταιρειών. Επίσης, καθιστά ευχερή –λόγω και της ύπαρξης των νέων τεχνολογιών– την πολυεπίπεδη ανάθεση της διαχείρισης των πληροφοριακών συστημάτων των εταιρειών. Δηλαδή μια εταιρεία μπορεί να αναθέτει την υποστήριξη/διαχείριση του πληροφοριακού της συστήματος σε τρίτους, οι οποίοι με τη σειρά τους, αναθέτουν μέρος της υπηρεσίας σε άλλους κ.ο.κ. Τα προσωπικά δεδομένα μπορούν έτσι να διακινούνται σε χώρες που δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας τους.

Και στην περίπτωση αυτή απαιτείται ένα νέο θεσμικό πλαίσιο, για την προστασία των προσωπικών δεδομένων, που θα μπορεί να αντιμετωπίσει τα νέα οικονομικά φαινόμενα. Στο σημείο αυτό θα ήθελα να υπογραμμίσω την ανάγκη διαμόρφωσης ενός ομοιόμορφου, διεθνούς θεσμικού πλαισίου. Η παγκοσμιοποιημένη οικονομία και οι νέες τεχνολογίες δεν μπορούν να αντιμετωπισθούν αποτελεσματικά μέσω εθνικών, ανομοιογενών ρυθμίσεων. Για το λόγο αυτό επιχειρείται από τις Αρχές Προστασίας Προσωπικών Δεδομένων η προώθηση σε διεθνές επίπεδο κανόνων για την προστασία των προσωπικών δεδομένων, όπως για παράδειγμα η ενθάρρυνση της υπογραφής και κύρωσης της Σύμβασης 108 και του Πρόσθετου Πρωτοκόλλου 181 του Συμβουλίου της Ευρώπης από τρίτες χώρες που δεν συμμετέχουν στο Συμβούλιο της Ευρώπης. Επίσης η Διεθνής Σύνοδος των Αρχών Προστασίας πρόκειται το Νοέμβριο του 2009 να υιοθετήσει ένα κείμενο που περιέχει ακριβώς τις βασικές αρχές, τα δικαιώματα και τις υποχρεώσεις σε σχέση με την προστασία των προσωπικών δεδομένων². Το κείμενο αυτό θα προωθηθεί στις κυβερνήσεις και τους υπευθύνους επεξεργασίας τρίτων χωρών. Ακόμη, ο Διεθνής Οργανισμός Προτυποποίησης (ISO) προωθεί αυτή τη στιγμή το υπ' αρ. 29100 τεχνικό πρότυπο «για ένα πλαίσιο προστασίας της ιδιωτικότητας στα πληροφοριακά και επικοινωνιακά συστήματα». Το πρότυπο αυτό παρουσιάζει ακόμη αρκετές αδυναμίες, κυρίως σε επίπεδο εννοιών, βρίσκεται όμως στη σωστή κατεύθυνση. Για το λόγο αυτό, όλες οι Αρχές Προστασίας Δεδομένων, και η ελληνική, υποστηρίζουμε ενεργώς την προσπάθεια και έχουμε αποστείλει σχόλια για τη βελτίωση του κειμένου.

2. Το κείμενο αυτό υιοθετήθηκε στις 6.11.2009 και είναι γνωστό ως η «Διακήρυξη της Μαδρίτης».

3. Ενίσχυση της δημόσιας ασφάλειας

Οι πολιτικές εξελίξεις, ιδίως η ανάγκη ενίσχυσης της δημόσιας ασφάλειας, και αντιμετώπισης της διεθνούς τρομοκρατίας και του διασυνοριακού εγκλήματος εντείνει τα μέτρα παρακολούθησης των πολιτών και οδηγεί στην προληπτική συλλογή και επεξεργασία όλο και περισσότερων προσωπικών δεδομένων.

Η νέα Συνθήκη της Λισαβώνας με το ενιαίο και όχι πλέον το τριγωνικό θεσμικό σχήμα των πυλώνων απαιτεί την επανεξέταση των προϋποθέσεων νόμιμης επεξεργασίας. Ειδικότερα, η «κοινοτικοποίηση» του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης προβλέπεται να προκαλέσει τα σοβαρότερα νομικά προβλήματα που θα κληθεί τελικά να επιλύσει το ΔΕΚ. Στα προβλήματα αυτά συγκαταλέγεται και το επίπεδο της προστασίας των προσωπικών δεδομένων που θα ισχύει στον ευρύτερο τομέα της ευρωπαϊκής, συνεπώς εν μέρει και εθνικής, ασφάλειας. Βεβαίως, ορισμένα βήματα έχουν ήδη γίνει: Υπάρχει η Απόφαση – Πλαίσιο του Συμβουλίου της ΕΕ (2008/977/ΔΕΥ, 27.11.2008) για την προστασία των προσωπικών δεδομένων στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις, δηλαδή στον τρίτο πυλώνα. Αυτή η Απόφαση προβλέπεται να εφαρμοστεί και μετά τη θέση σε ισχύ της Συνθήκης της Λισαβώνας.

Γενικότερα, όσον αφορά στα μέτρα για τη δημόσια ασφάλεια θα ήθελα να επισημάνω ότι ένα μέτρο που περιορίζει τα ατομικά δικαιώματα πρέπει να υπακούει στην αρχή της αναλογικότητας, δηλαδή να είναι πρόσφορο και πραγματικά αναγκαίο, όχι απλώς χρήσιμο, για την επίτευξη της δημόσιας ασφάλειας και βεβαίως να θεσπίζεται με νόμο. Στην ελληνική έννομη τάξη απαιτείται τυπικός νόμος ή κατόπιν ειδικής νομοθετικής εξουσιοδότησης προεδρικό διάταγμα. Κατά την πάγια νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), ο νόμος πρέπει να παρουσιάζει ορισμένα ποιοτικά χαρακτηριστικά, όπως είναι, μεταξύ άλλων η προβλεψιμότητα των συνεπειών του (foreseeability). Ο σεβασμός των νομολογιακών κατευθύνσεων του ΕΔΔΑ αποτελεί πλέον καταγεγραμμένο στόχο της ελληνικής δημόσιας διοίκησης στο πρόγραμμα για τη «Διοικητική Μεταρρύθμιση».

Δυστυχώς, όμως, προσφάτως θεσπίστηκαν, με τη διαδικασία της τροπολογίας, δύο νομοθετικές ρυθμίσεις για την εγκατάσταση καμερών σε δημόσιους χώρους και τη δημιουργία εθνικής βάσης γενετικών αποτυπωμάτων (DNA), που δεν εξασφαλίζουν τις απαραίτητες εγγυήσεις για την προστασία των ατομικών δικαιωμάτων. Η ΑΠΔΠΧ είχε την ευκαιρία να γνωμοδοτήσει³ σχετικά με τις δύο τροπολογίες και να καταγράψει, με μία σειρά παρατηρήσεων, τα προβλήματα συνταγματικότητας και συμβατότητας προς την ΕΣΔΑ των νέων ρυθμίσεων.

Η Αρχή δεν αρνήθηκε τη νομική δυνατότητα εγκατάστασης κλειστών κυκλωμάτων τηλεόρασης σε δημόσιους χώρους με σκοπό την πρόληψη και καταστολή της εγκληματικότητας, αλλά ανέδειξε την ανεπάρκεια της ρύθμισης από απόψεως προστασίας των προσωπικών δεδομένων, μιας ρύθμισης που περιορίζεται στην αφαίρεση από την ελεγκτική αρμοδιότητα της Αρχής ενός μεγάλου και ευαίσθητου τομέα της κρατικής δράσης.

Ομοίως η Αρχή, ακολουθώντας τη νομολογία του ΕΔΔΑ, δέχθηκε ότι η χρήση γενετικών αναλύσεων και η δημιουργία αρχείου γενετικών αποτυπωμάτων για την εξιχνίαση αξιόποινων πράξεων αποτελεί καταρχήν ένα θεμιτό σκοπό επεξεργασίας προσωπικών δεδομένων. Ωστόσο επισήμανε ότι η συγκεκριμένη ρύθμιση δεν εναρμονίζεται με τις επιταγές του άρθρου 9Α του Συντάγματος και του άρθρου 8 της ΕΣΔΑ, διότι δεν τηρούνται οι αρχές της νομιμότητας και της αναλογικότητας, καθώς και το τεκμήριο αθωότητας.

4. Συμπέρασμα

Αν πρέπει να ολοκληρώσω την ομιλία μου με ένα συμπέρασμα, θα έλεγα επιγραμματικά ότι οι προκαλούμενοι κίνδυνοι, από τις νέες τεχνολογίες, την παγκοσμιοποιημένη οικονομία και την ανάγκη ενίσχυσης της δημόσιας ασφάλειας, μπορούν να αντιμετωπισθούν, σε διεθνές και εθνικό επίπεδο, με τις κατάλληλες νομοθετικές πρωτοβουλίες και τεχνολογικές εφαρμογές, χωρίς υπέρμετρους περιορισμούς των ατομικών δικαιωμάτων.

3. Γνωμοδοτήσεις 1 και 2/2009, διαθέσιμες σε: www.dpa.gr

* * * * *