ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

Βαγγέλης Παπακωνσταντίνου

Ψηφιακη Ελλαδα

- ιστορική διαδρομή
- σύγχρονο ρυθμιστικό πλαίσιο
- προτάσεις για το μέλλον

Πίνακας Περιεχομένων

Η επεξεργασία δεδομένων του προσωπικού χαρακτήρα

Το Δίκαιο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα δεν είναι ένας τομέας δικαίου με μεγάλη ιστορία: τα πρώτα νομοθετήματα έκαναν την εμφάνισή τους στη Γερμανία μόλις κατά τη δεκαετία του 1960, και μάλιστα κατά τα τέλη της. Οι λόγοι που δημιουργήθηκε είχαν να κάνουν με τις νέες τεχνολογίες πληροφορικής και τηλεπικοινωνιών που τότε ξεκίνησαν και εκείνες να κάνουν αισθητή την παρουσία τους. Μέσα όμως σε μόλις 50 χρόνια ό,τι ξεκίνησε ως ένας μόνο νόμος, αποτέλεσμα ίσως της υπερευαισθησίας μερικών κρατών με ανεπτυγμένο τεχνολογικό επίπεδο και νωπές ιστορικές μνήμες, εξελίχθηκε σε τομέα δικαίου με –χωρίς υπερβολή– καθημερινές εφαρμογές στη ζωή οποιουδήποτε έχει και στοιχειώδη έστω σχέση με τις νέες τεχνολογίες και τη σύγχρονη ζωή.

Σήμερα δεδομένα προσωπικού χαρακτήρα μεταδίδονται και συλλέγονται κάθε λεπτό της ζωής μας: όποτε περπατάμε σε δρόμους παρακολουθούμενους από CCTV κάμερες, πάμε στο γραφείο μας όπου λειτουργούν εξίσου κάμερες ασφαλείας, ψωνίζουμε στο σούπερ μάρκετ, συναλλασσόμαστε στο Διαδίκτυο, χρησιμοποιούμε τις πιστωτικές μας κάρτες κ.ο.κ. Το άτομο σήμερα, στην Ελλάδα τουλάχιστον, σπάνια περνά περισσότερες από λίγες ώρες οποιασδήποτε μέρας του που να μην εκτελεί δραστηριότητες που ρυθμίζονται από το Δίκαιο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Στην Ελλάδα αργήσαμε και τελικά υποχρεωθήκαμε από τους Κοινοτικούς μας Εταίρους να αποκτήσουμε Δίκαιο Προστασίας Δεδομένων. Από το 1997 πάντως και μετά συμμετέχουμε και εμείς στην κίνηση αυτή και σήμερα, με τον έναν ή τον άλλον τρόπο, τα δεδομένα προσωπικού χαρακτήρα έχουν μπει στο λεξιλόγιο καθενός μας, ανεξαρτήτως αν έχει σχέση με τις νέες τεχνολογίες ή όχι.

Στο σημείο αυτό τρεις απαραίτητες διευκρινίσεις πριν την επιμέρους, επιλεκτική, ανάλυση κάποιων παραμέτρων του Δικαίου Προστασίας Δεδομένων από την οπτική του χρήστη που ακολουθεί παρακάτω: η πρώτη αφορά τη συμμετοχή μας στην ΕΕ. Η Ελλάδα και στον τομέα αυτόν επωφελείται από Δίκαιο που παράγεται στην Κοινότητα και το οποίο απλά καλείται να εφαρμόσει στο εσωτερικό της (και τιμωρείται αν δεν το κάνει ή το κάνει με άλλον τρόπο από εκείνον που επιθυμούν οι Βρυξέλλες). Ευτυχώς, γιατί όπως θα καταδειχθεί όσες φορές οι Έλληνες νομοθέτες/κυβερνήσεις αφέθηκαν να νομοθετήσουν μόνοι τους τα αποτελέσματα ήταν καταστροφικά για το άτομο. Επιπλέον, το νομικό μας σύστημα με τον τρόπο αυτό, μέσω δηλαδή Βρυξελλών, εκσυγχρονίζεται και προβληματίζεται για εξελίξεις στις τεχνολογίες, στο μάρκετινγκ, στη διεθνή πολιτική σκηνή και αλλού, ενέργειες που η χώρα, ακόμα και αν ποτέ υποτεθεί ότι θα ήθελε να κάνει, προφανώς δεν διαθέτει τα μέσα να το κάνει το ίδιο καλά με την Κοινότητα. Κατά συνέπεια, βέβαια, η «ανεξαρτησία» του έλληνα νομοθέτη, της ελληνικής κυβέρνησης, της ελληνικής Αρχής Προστασίας Δεδομένων ή και των ελληνικών δικαστηρίων έχει, στην ουσία, χαθεί.

Η δεύτερη διευκρίνιση αφορά το πεδίο εφαρμογής του Δικαίου Προστασίας Δεδομένων. Ο νέος τομέας δικαίου δημιουργήθηκε περίπου πενήντα χρόνια πίσω, ως απάντηση στην αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα που τότε ξεκινούσε και υπό τον εφιάλτη του οργουελιανού Big Brother. Στο μεσοδιάστημα, και παρά τις τεχνολογικές και μάλιστα υπολογιστικές του καταβολές, το πεδίο εφαρμογής του διευρύνθηκε ώστε να περιλάβει όλα τα δεδομένα που τηρούνται σε «αρχείο», ανεξαρτήτως της ύπαρξης υπολογιστή. Έτσι, παρότι το δικαίωμα προστασίας δεδομένων (data protection) ξεκίνησε τη σταδιοδρομία του ως υποσύνολο του δικαιώματος προστασίας της ιδιωτικής ζωής (right to privacy), στην κοινή (και όχι μόνο) συνείδηση τα δύο δικαιώματα ταυτίστηκαν, ακριβώς επειδή το πρώτο είναι καλύτερα εξοπλισμένο για να ανταποκριθεί στη σύγχρονη, ηλεκτρονική, πραγματικότητα.

Με τον τρόπο βέβαια αυτό σήμερα φτάσαμε στην υπερβολή δεδομένα προσωπικού χαρακτήρα να θεωρούνται σχεδόν τα πάντα, ακόμα και ένα ονοματεπώνυμο γραμμένο με το χέρι σε ένα κομμάτι χαρτί. Αν μάλιστα στη συνέχεια το τσαλακώσουμε και το πετάξουμε θα έχουμε προβεί σε «διαγραφή», δηλαδή σε «επεξεργασία» κατά το νόμο!

Οι συνέπειες αυτής της τάσης (Κοινοτικής, δεν πρέπει να κατηγορούνται μόνο οι Έλληνες νομοθέτες και εφαρμοστές του νόμου γι' αυτήν) είναι περισσότερες, δύο όμως μόνο σημειώνονται εδώ. Από νομική άποψη, φαίνεται τελικά πως, κακώς μεν, το τεκμήριο κάθε φορά είναι υπέρ της εφαρμογής του Δικαίου Προστασίας Δεδομένων σε περιπτώσεις αμφιβολίας. Από πρακτική

άποψη η γιγάντωση αυτή του πεδίου εφαρμογής δεν είναι απαραίτητο ότι πράγματι βοηθά τον πολίτη: οι επεξεργασίες σήμερα είναι τόσες πολλές και οι πόροι της Αρχής Προστασίας Δεδομένων τόσο περιορισμένοι που αντί για διεύρυνση μάλλον περιορισμό των αρμοδιοτήτων της θα έπρεπε να ζητά.

Η τρίτη διευκρίνιση αφορά τον «πόλεμο κατά της τρομοκρατίας». Όταν μιλάμε για το Δίκαιο Προστασίας Δεδομένων πρέπει να διακρίνουμε μεταξύ της προ και μετά-9/11 εποχής. Μετά την 11η Σεπτεμβρίου 2001 και την επίθεση στους Δίδυμους Πύργους στη Νέα Υόρκη τα πάντα που αφορούσαν το Δίκαιο Προστασίας Δεδομένων άλλαξαν. Μέχρι εκείνη την ημέρα ζητούμενο ήταν πρώτα η προστασία του πολίτη και έπειτα η εκτέλεση της επεξεργασίας, συνήθως μάλιστα για εμπορικούς σκοπούς. Από την ημέρα εκείνη και μετά το ζητούμενο ήταν, και παραμένει, πρώτα η εκτέλεση όσο το δυνατόν περισσότερο εκτεταμένων επεξεργασιών για λόγους ασφαλείας και έπειτα η μη προσβολή του δικαιώματος του πολίτη στα δεδομένα του. Εννοείται επίσης ότι τώρα πια οι επεξεργασίες γίνονται κυρίως όχι για εμπορικούς σκοπούς, αλλά από κρατικές αρχές ασφαλείας. Αυτή η εξέλιξη θα αλλάξει για πάντα το Δίκαιο Προστασίας Δεδομένων. Παρότι μέσω της παραδοχής του ως παίκτη στο παιχνίδι της διεθνούς κρατικής ασφάλειας εξασφαλίζει τη συνεχιζόμενη ύπαρξή του, το ακριβές του περιεχόμενο περιορίζεται και υποτάσσεται σε σκοπούς τους οποίους ακριβώς δημιουργήθηκε για να περιορίσει.

Πώς και έχουμε Δίκαιο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;

Το Δίκαιο Προστασίας Δεδομένων, όπως ήδη αναφέρθηκε, δεν είναι ιδιαίτερα παλαιό: μόλις κατά τα τέλη της δεκαετίας του 1960 έκαναν την εμφάνισή τους οι πρώτοι αντίστοιχοι (βασικοί) νόμοι, στα κρατίδια της τότε Ομοσπονδιακής Δημοκρατίας της Γερμανίας. Οι λόγοι που οδήγησαν στην γένεση των νόμων αυτών είναι απλοί: μόλις κατά τα χρόνια εκείνα οι υπολογιστές βγήκαν από τα ακαδημαϊκά εργαστήρια και μπήκαν στη δημόσια διοίκηση (μόνο εκεί αρχικά, λόγω κόστους).

Όταν όμως άρχισε η οργάνωση των στοιχείων των πολιτών σε καρτέλες υπολογιστών αντί σε φακέλους από χαρτί, όπως γινόταν μέχρι τότε, έγιναν αμέσως φανερές σε όλους οι τεράστιες νέες δυνατότητες επεξεργασίας που το νέο μέσο προσέφερε στους ιδιοκτήτες του. Ενώ παλαιότερα η απάντηση σε απλά ερωτήματα του τύπου «ποιοι μένουν στην οδό τάδε» ή «ποιοι λαμβάνουν το βοήθημα τάδε» ή «ποιοι είναι υπηκοότητας δείνα» απαιτούσε επίπονη εργασία διασταύρωσης πολλών εγγράφων που αναγκαστικά γινόταν χειρονακτικά, ξαφνικά η πληροφορία ερχόταν έτοιμη σε δευτερόλεπτα. Οι νέες δυνατότητες επεξεργασίας και συνδυασμών των ατομικών στοιχείων των πολιτών έκοβαν την ανάσα σε σχέση με το παρελθόν.

Αυτό ακριβώς το κόψιμο της ανάσας επανέφερε μνήμες ολοκληρωτικών καθεστώτων του πρόσφατου παρελθόντος. Ας μην ξεχνάμε ότι η Ευρώπη μόλις είχε τελειώσει τον Δεύτερο Παγκόσμιο Πόλεμο. Οι γενιές ήταν ίδιες, η ίδια γενιά που πολέμησε ήταν στα πράγματα και το 1960. Οι μνήμες της ναζιστικής Γερμανίας και των οργανωμένων διώξεων των Εβραίων ήταν ακόμα νωπές. Σε πολλά κράτη της Ευρώπης οι Γερμανοί κατακτητές επωφελήθηκαν από την άρτια διοικητική τους οργάνωση για να ψάξουν στα κρατικά αρχεία και να εντοπίσουν τους Εβραίους πολίτες. Η ίδια η Γερμανία έφερε ακόμα τις περισσότερες πληγές από το παρελθόν αυτό. Εύλογα λοιπόν, όταν ο πρώτος υπολογιστής μπήκε στη δημόσια διοίκηση (σε τοπικές κυβερνήσεις κρατιδίων της Ομοσπονδιακής Γερμανίας), οι κυβερνήσεις αυτές διέγνωσαν τις δυνατότητες του νέου μέσου για την παρακολούθηση του ατόμου και αποφάσισαν ότι κάτι έπρεπε να γίνει γι' αυτό.

Από τη στιγμή που τα πρώτα γερμανικά κρατίδια απέκτησαν νόμο για την προστασία των δεδομένων προσωπικού χαρακτήρα η μόδα διαδόθηκε. Πρώτο εθνικό νομοθέτημα απέκτησε η Σουηδία, ενώ κατά τη δεκαετία του 1970 ακολούθησαν πλήθος άλλα, τεχνολογικά ανεπτυγμένα κράτη, από την ίδια τη Γερμανία σε ομοσπονδιακό επίπεδο και τη Γαλλία μέχρι τις ΗΠΑ. Σε αυτή την εξέλιξη βοήθησε και το γενικότερο κλίμα, αφού όπως είναι γνωστό κατά τις δεκαετίες 1960 και 1970 υπήρχε ενθουσιασμός για τα ανθρώπινα δικαιώματα (και αντίπαλος παρέμενε το κράτος), αλλά και η μόδα: πράγματι, μια διεθνής ομάδα «φίλων» (πολιτικών, ακαδημαϊκών, ακτιβιστών κ.λπ.) που κινούνταν σε υψηλό επίπεδο στις χώρες καταγωγής της φρόντισε ώστε ένα ένα τα τεχνολογικά ανεπτυγμένα κράτη να αποκτήσουν αντίστοιχο νόμο.

Στις αρχές της δεκαετίας του 1980 μόνο το Ηνωμένο Βασίλειο, και η συντηρητική τότε κυβέρνηση Θάτσερ, αντιστεκόταν πεισματικά στη νέα τάση. Αποφασιστικής σημασίας για να καμφθεί η αντίστασή του ήταν η βασική αρχή του Δικαίου Προστασίας Δεδομένων, που θα αναλυθεί παρακάτω, περί μη εξαγωγής δεδομένων σε τρίτες χώρες που δεν εξασφαλίζουν επίπεδο προστασίας «αντίστοιχο» με το εθνικό. Επειδή η αγγλική οικονομία θα στερούνταν ξαφνικά τη δυνατότητα συνεργασίας με τη γαλλική ή τη γερμανική (αφού δεδομένα δεν θα κινούνταν προς αυτήν), έτσι πείστηκε και το Ηνωμένο Βασίλειο μόλις το 1984.

Στη συνέχεια δεν είχαν λόγο να μην ακολουθήσουν και οι Ολλανδία και Ιρλανδία (σε αυτή την ταχύτητα θα βρισκόταν και η Ελλάδα που μέσω του καθηγητή Σπύρου Σημίτη συμμετείχε, αν δεν διαμόρφωνε κιόλας, την παραπάνω «διεθνή ομάδα» από τη γερμανική βέβαια πλευρά, αλλά η πρωτοβουλία απέτυχε για άσχετους λόγους εσωτερικής πολιτικής).

Η δεκαετία του 1980 σηματοδότησε την αλλαγή προσανατολισμού του Δικαίου Προστασίας Δεδομένων από την άμυνα έναντι του κράτους στην ά-

μυνα έναντι του ιδιωτικού τομέα. Όπως οι παλαιότεροι από εμάς θυμούνται τότε ήταν που οι τιμές των υπολογιστών έπεσαν σε προσιτά επίπεδα για πρώτη φορά: τότε ζήσαμε την έκρηξη των PCs και τα πρώτα Windows. Επιχειρήσεις άρχισαν την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς μάρκετινγκ και βελτίωσης των πωλήσεών τους, πολλές φορές και με αθέμιτα μέσα. Λίστες με δεδομένα προσωπικού χαρακτήρα άρχισαν να αποτελούν αντικείμενο οικονομικών συναλλαγών. Ο αντίπαλος για το άτομο έγινε ο ιδιωτικός τομέας, και λιγότερο πλέον το Κράτος.

Επόμενο στάδιο εξέλιξης του Δικαίου Προστασίας Δεδομένων ήταν φυσικά η Οδηγία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα το 1994. Μόλις κατά τις αρχές του 1990, η Ευρωπαϊκή Επιτροπή αντιλήφθηκε ότι όλα τα Κράτη-Μέλη (πλην Ιταλίας και Ελλάδας) είχαν εθνικούς νόμους για την προστασία δεδομένων, σκέφτηκε ότι έπρεπε να δράσει ώστε να δημιουργηθεί κοινό πλαίσιο στο πλαίσιο και της Ενιαίας Αγοράς. Μετά από πολυετείς διαπραγματεύσεις οριστικοποιήθηκε το κείμενο της Οδηγίας, την οποία ενσωμάτωσε και η Ελλάδα στο εθνικό της δίκαιο, και η οποία τελικά δεν είναι τίποτα άλλο παρά ένας συμβιβασμός μεταξύ του γερμανικού, του γαλλικού και του αγγλικού εθνικού μοντέλου προστασίας δεδομένων.

Βέβαια, και πάλι η Ιστορία αποδείχθηκε αμείλικτος κριτής. Παρότι κανείς δεν θα μπορούσε να αμφισβητήσει τη σημασία της Οδηγίας και πόσο απαραίτητη ήταν τότε που δημιουργήθηκε, γεγονός παραμένει ότι η Οδηγία, ως Οδηγία, ρύθμισε μόνο εμπορικο-οικονομικές επεξεργασίες. Η Ευρωπαϊκή Επιτροπή που εξέδωσε την Οδηγία δεν μπορούσε να ρυθμίσει τις ποινικές επεξεργασίες ή τις επεξεργασίες εθνικής ασφάλειας διότι κάτι τέτοιο δεν ανήκει στις αρμοδιότητές της. Το Συμβούλιο της Ευρώπης, που πράγματι έχει αυτήν την αρμοδιότητα, είχε εκδώσει Συνθήκη ήδη από το 1984, αλλά το κείμενό της δέκα χρόνια μετά ήταν ήδη παρωχημένο (πολύ περισσότερο μάλιστα σήμερα, που συνεχίζει να ισχύει).

Έτσι, οι αντικειμενικά πλήρεις κανόνες της Οδηγίας αφορούν μόνο τις εμπορικές επεξεργασίες, άσχετο αν κάποια Κράτη Μέλη κατά την ενσωμάτωσή τους στο εθνικό τους δίκαιο διάλεξαν να ρυθμίσουν και άλλες επιπλέον επεξεργασίες π.χ. της Αστυνομίας. Κατά τη δεκαετία του 1990 αυτή η διάκριση δεν δημιουργούσε πρόβλημα, και μάλιστα κανείς δεν ασχολούνταν μαζί της. Σήμερα, μετά την 9/11 και την ανάγκη ρύθμισης των επεξεργασιών δεδομένων προσωπικού χαρακτήρα για σκοπούς ασφαλείας («πόλεμος κατά της τρομοκρατίας»), γίνεται φανερό ότι πολύ καλύτερα θα ήταν αν το νομικό πλαίσιο είχε δημιουργηθεί από τότε, μαζί με την Οδηγία, όταν ο κόσμος ήταν σε νηφαλιότητα και όχι ήδη σε πόλεμο και φοβούμενος τυφλά χτυπήματα τρομοκρατών.

Σε κάθε περίπτωση κατά τα μέσα και τέλη της δεκαετίας του 1990 υπήρχε ενθουσιασμός με το κείμενο της Οδηγίας: όλα τα Κράτη-Μέλη είχαν πλέον κοινό νόμο (και η Ελλάδα και η Ιταλία), η Κοινότητα διέθετε Κοινοτικά Όργανα (την Ομάδα του Άρθρου 29) και τα μόνα προβλήματα νομίζαμε ότι ήταν πώς θα πείσουμε τις ΗΠΑ να συνεργαστούν (που μετά τον πρώτο νόμο του 1974 για δικούς τους εσωτερικούς λόγους δεν ακολούθησαν τη διεθνή τάση ενίσχυσης του δικαιώματος στην ιδιωτικότητα με το δικαίωμα προστασίας δεδομένων).

Όλα άλλαξαν μετά την 9/11. Πρώτες οι ΗΠΑ και πλέον και ευρωπαϊκά Κράτη-Μέλη απαιτούν να μπορούν να επεξεργάζονται μαζικά δεδομένα προσωπικού χαρακτήρα στην προσπάθεια να βελτιώσουν τον κρατικό τους μηχανισμό ασφαλείας και να αποφύγουν ένα ακόμα τρομοκρατικό χτύπημα στο εσωτερικό τους. Η τάση, δυστυχώς, διεθνώς είναι στάση κατανόησης προς τη θέση αυτή. Από εκεί που υπήρχε ενθουσιασμός για το δικαίωμα του πολίτη να ελέγχει ο ίδιος τη ροή των δεδομένων που τον αφορούν (δικαίωμα πληροφοριακού αυτοκαθορισμού), σήμερα υπάρχει ενθουσιασμός για τις νέες υπολογιστικές δυνατότητες της Αστυνομίας.

Το διεθνές κλίμα είναι προφανώς μη αναστρέψιμο, και νέα ρυθμιστικά κείμενα εκδίδονται συνεχώς που, παρότι κατ' όνομα εντάσσονται στο Δίκαιο Προστασίας Δεδομένων, κάθε άλλο παρά τα δεδομένα των πολιτών προστατεύουν. Και αυτό δεν είναι το χειρότερο – αν οι επεξεργασίες που τώρα γίνονται επιτρεπτές σχετίζονταν μόνο με την τρομοκρατία, το πρόβλημα θα ήταν μικρό. Το πρόβλημα αντιθέτως διογκώνεται από το γεγονός ότι η τρομοκρατία στην ουσία αποτελεί σήμερα την κερκόπορτα για την άλωση του συνόλου των ανθρώπινων δικαιωμάτων. Πράγματι, όπως θα δούμε παρακάτω, η τρομοκρατία είναι μόνο η αφορμή: κάθε φορά που νέος νόμος θέτει σε εκκίνηση τη νομοθετική διαδικασία για την καταπολέμηση της τρομοκρατίας στην Κοινότητα υπάρχουν πάντα εκείνοι που κατά τη διαδικασία οριστικοποίησής του αντικαθιστούν το «τρομοκρατία» με το «σοβαρό έγκλημα» και στη συνέχεια με σκέτο «έγκλημα» –τα καταστροφικά αποτελέσματα των αντικαταστάσεων αυτών είναι φανερά σε καθέναν μας.

Ποιο είναι το σύστημα οργάνωσής του;

Το Δίκαιο Προστασίας Δεδομένων λειτουργεί, δυστυχώς, λιγότερο ή περισσότερο βάσει του ίδιου συστήματος που επινοήθηκε κατά τη δεκαετία του 1960, παρά την κοσμογονία που έχει συμβεί στο μεταξύ. Θεμελιώδες δομικό του στοιχείο είναι ο βασικός νόμος που το εισάγει στο νομικό σύστημα κάθε χώρας και το οριοθετεί: στην Ευρώπη τον ρόλο αυτόν για την ώρα τον έχει η Οδηγία, στην Ελλάδα ο Νόμος για την Προστασία του Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα (ν.2472/1997, όπως έχει έκτο-

τε τροποποιηθεί και ισχύει σήμερα). Συχνά το Δίκαιο Προστασίας Δεδομένων έχει την τύχη και συνταγματικής κάλυψης: αυτό, για παράδειγμα, ισχύει στην Ελλάδα, όπου το δικαίωμα «προστασίας προσωπικών (sic) δεδομένων» κατοχυρώνεται στο κείμενο του νέου Συντάγματος, στο άρθρο 9Α: «*καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει*». Το ίδιο δικαίωμα άλλωστε περιλαμβάνεται και στον Ευρωπαϊκό Χάρτη Θεμελιωδών Δικαιωμάτων (Άρθρο 8).

Ο βασικός νόμος του Δικαίου Προστασίας Δεδομένων διακρίνεται σε δύο μέρη: στο πρώτο περιλαμβάνονται οι ουσιαστικές διατάξεις του Δικαίου Προστασίας Δεδομένων και στο δεύτερο ιδρύεται ανεξάρτητος οργανισμός με κρατική εγγύηση (ανεξάρτητη διοικητική αρχή – η Αρχή Προστασίας Δεδομένων, στην Ελλάδα) που εφαρμόζει τις διατάξεις του νόμου στο εσωτερικό της χώρας και συνεργάζεται διεθνώς όπου χρειαστεί.

Το σύστημα του Δικαίου Προστασίας Δεδομένων στηρίζεται σε τέσσερις πυλώνες: στις βασικές αρχές επεξεργασίας των δεδομένων, στα βασικά δικαιώματα που δίνονται στους πολίτες, στο σύστημα της γνωστοποίησης, και στην ίδρυση της Αρχής Προστασίας Δεδομένων για τον έλεγχο καλής εφαρμογής των προηγούμενων.

Οι βασικές αρχές επεξεργασίας αποτελούν ίσως μοναδική περίπτωση νομοθετικής επιτυχίας στον τομέα των νέων τεχνολογιών. Επινοήθηκαν στα τέλη της δεκαετίας του 1960, παραμένουν απαράλλακτες μέχρι σήμερα και οι διατάξεις τους είναι περισσότερο επίκαιρες παρά ποτέ. Παρά την τεχνολογική κοσμογονία, τη γενίκευση χρήσης υπολογιστών, την έλευση του Διαδικτύου, τα δίκτυα επικοινωνίας, αλλά και την 9/11, κάθε μια από τις αρχές αυτές ακούγεται σήμερα σύγχρονη και στην καρδιά των ζητημάτων. Οι αρχές αυτές είναι η αρχή της συλλογής και επεξεργασίας των δεδομένων με νόμιμο και θεμιτό τρόπο, η αρχή της δεσμευτικότητας του σκοπού της επεξεργασίας, η αρχή της συνάφειας και της ποιότητας των δεδομένων, της ασφάλειας των δεδομένων, του απόρρητου της επεξεργασίας και της πεπερασμένης διατήρησης των δεδομένων.

Το ίδιο ακριβώς ισχύει και για τον δεύτερο πυλώνα του συστήματος του Δικαίου Προστασίας Δεδομένων. Προκειμένου το άτομο να προστατευτεί καλύτερα κατά την επεξεργασία των δεδομένων του εξοπλίζεται με ειδικό «σετ» δικαιωμάτων: το δικαίωμα ενημέρωσης (ότι τελείται επεξεργασία δεδομένων του), το δικαίωμα πρόσβασης (στα δεδομένα του που έχουν αποτελέσει αντικείμενο επεξεργασίας) και το δικαίωμα διόρθωσης (αν κατά την πρόσβασή του σε αυτά διαπιστώσει λάθος). Χωρίς αυτά τα ειδικά δικαιώματα, μόνο με

το δικαίωμα καταφυγής στα δικαστήρια (που ούτως ή άλλως έχει), το άτομο θα εγκαταλειπόταν αβοήθητο σε ένα περιβάλλον επεξεργασίας που γίνεται όλο και πιο σύνθετο.

Ο τρίτος πυλώνας του συστήματος του Δικαίου Προστασίας Δεδομένων, σε αντίθεση με τα παραπάνω, είναι δυστυχώς παρωχημένος. Ο νομοθέτης του 1960 είχε άλλον «υπολογιστή» στο μυαλό του από ό,τι ισχύει σήμερα, αφού άλλωστε από την εποχή των πανάκριβων, μοναδικών μεγάλων υπολογιστικών συστημάτων (mainframes) φτάσαμε στην εποχή της νεφοϋπολογιστικής (cloud computing). Όμως το 1960 ο νομοθέτης φανταζόταν ότι επεξεργασίες θα γίνονταν περιορισμένα και από λίγους επομένως εισήγαγε Μητρώο όπου όλες θα καταγράφονταν, ώστε να παρακολουθούνται ευχερέστερα από τις εποπτικές αρχές. Έτσι, βάσει της υποχρέωσης «γνωστοποίησης» του υπεύθυνου επεξεργασίας, κάθε επεξεργασία στο εσωτερικό της χώρας πρέπει να καταγράφεται λεπτομερώς σε Μητρώο που τηρεί στα γραφεία της η εποπτική αρχή.

Η πραγματικότητα, ως γνωστόν, αποδείχτηκε εντελώς διαφορετική. Σήμερα επεξεργασίες κάνουμε όλοι, από τον χρήστη κινητού τηλεφώνου που επεξεργάζεται τις επαφές του, μέχρι τις τράπεζες, τα νοσοκομεία, τις ασφαλιστικές εταιρείες, τους διαδικτυακούς τόπους κ.ο.κ. Σε αυτό το πλαίσιο η καταγραφή όλων των επεξεργασιών είναι πρακτικά και θεωρητικά αδύνατη. Παρ' όλα αυτά το σύστημα, αντί να αντικατασταθεί, έχει γίνει προσπάθεια να διατηρηθεί τεχνητά στη ζωή: προκειμένου να αποφευχθεί να πάει όλη η Ελλάδα στην Αρχή να δηλωθεί, μεγάλες κατηγορίες αυτονόητων επεξεργασιών εξαιρέθηκαν (π.χ. επεξεργασίες του μισθολογίου, του πελατολογίου κ.ο.κ.). Για άλλες πάλι κατηγορίες επεξεργασιών κανόνες ειδικοί γι' αυτές τις εξαιρούν συνολικά (η δυνατότητα αυτή πάντως δεν έχει εφαρμοστεί ακόμα στην Ελλάδα). Γενικά όμως το σύστημα της γνωστοποίησης, παρά τη μηδενική χρησιμότητά του σήμερα, στην πράξη εξακολουθεί να μένει ενεργό.

Ο τέταρτος πυλώνας αφορά την ίδρυση εποπτικής αρχής. Ο οργανισμός αυτός ευθύς αμέσως αποφασίστηκε ότι θα έπρεπε να είναι ανεξάρτητος (αφού, μην ξεχνάμε, αρχικά το Κράτος ήταν ο αντίπαλος) και αυτοδιοικούμενος. Ο χαρακτήρας του πάντως μπορεί να ποικίλλει σε οτιδήποτε από δικαστοκρατικός (όπως π.χ. στην Ελλάδα) μέχρι επικοινωνιακός (όπως π.χ. στο Ηνωμένο Βασίλειο). Σε κάθε περίπτωση, στον οργανισμό αυτόν ανατέθηκε αποκλειστικό έργο η παρακολούθηση της εφαρμογής του νόμου στο εσωτερικό κάθε χώρας. Στο μεταξύ βέβαια οι επεξεργασίες γενικεύτηκαν, και οι οργανισμοί αυτοί σήμερα καλούνται να παρακολουθήσουν ειδικευμένες επεξεργασίες από τράπεζες μέχρι μαιευτήρια και CCTV κάμερες στους δρόμους με πενιχρά μέσα –περισσότερα όμως γι' αυτό παρακάτω.

Ο βασικός νόμος του Δικαίου Προστασίας Δεδομένων συμπληρώνεται από πλήθος άλλων ειδικών νόμων, ειδικών άρθρων σε νόμους που εν μέρει περιλαμβάνουν επεξεργασίες δεδομένων προσωπικού χαρακτήρα, Αποφάσεων της Αρχής Προστασίας Δεδομένων, κωδίκων δεοντολογίας και άλλων ρυθμίσεων διαφορετικής κάθε φορά τυπικής ισχύος. Σε αυτούς πρέπει, για την Ελλάδα, να προστεθεί και όλη η Κοινοτική εργασία: Οδηγίες, Αποφάσεις-Πλαίσιο, Κανονισμοί, Γνωμοδοτήσεις, αποφάσεις του ΔΕΕ, όλα βρίσκουν εφαρμογή με τον έναν ή τον άλλον τρόπο στο εσωτερικό των Κρατών-Μελών. Τέλος, δεν πρέπει να παραβλέπεται και η νομολογία εθνικών δικαστηρίων άλλων Κρατών-Μελών: από τη στιγμή που όλοι μας εντός της Κοινότητας εφαρμόζουμε το ίδιο βασικά δίκαιο (εξαιτίας της Οδηγίας), είναι φανερό ότι αποφάσεις για κάποιο ζήτημα ενός, για παράδειγμα, γερμανικού ή ιταλικού δικαστηρίου επηρεάζουν και τον έλληνα δικαστή –και αντίστροφα.

Πώς λειτουργεί στην πράξη για τον μέσο Έλληνα;

Ο μέσος Έλληνας, χρήστης ή μη νέων τεχνολογιών, δεν περνά ώρα της ημέρας του που να μην εμπλέκεται σε δραστηριότητα δυνητικά ρυθμιζόμενη από το Δίκαιο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Στο σπίτι του χρησιμοποιεί το Διαδίκτυο (περιλαμβανομένης της VOIP τηλεφωνίας ή της IPTV τηλεόρασης). Στην εργασία του χτυπά κάρτα, πληρώνεται απευθείας σε τραπεζικό λογαριασμό, αν δεν παρακολουθείται κιόλας η είσοδος και έξοδός του από το κτήριο με κάμερες. Στο δρόμο παρακολουθείται από σωρεία καμερών, από τις CCTV της Αστυνομίας μέχρι τις κάμερες στις τράπεζες (και στα ATM) ή στις καφετέριες. Ψωνίζει με τη χρήση πιστωτικής κάρτας, στέλνει SMS μηνύματα και τηλεφωνεί με το κινητό του, συμμετέχει σε διαφημιστικές εκστρατείες κ.ο.κ. Όλες οι παραπάνω δραστηριότητες περιλαμβάνουν την παράδοση των δεδομένων του προσωπικού χαρακτήρα σε τρίτους, εντός ή και εκτός της χώρας.

Εξίσου πολλές επεξεργασίες συμβαίνουν στο παρασκήνιο: δεδομένα του επεξεργάζονται κάθε λεπτό π.χ. εταιρείες τηλεφωνίας για να εκδώσουν τους λογαριασμούς τους, εταιρείες πιστωτικών καρτών για τους αντίστοιχους δικούς τους, το Δημόσιο για τους δικούς του σκοπούς, εταιρείες άμεσου μάρκετινγκ (direct marketing) και πλήθος άλλοι. (Και) ο μέσος Έλληνας βρίσκεται στην ουσία μπλεγμένος σε δίχτυ επεξεργασιών στις οποίες ο ίδιος συμμετέχει ενεργητικά ή παθητικά και οι οποίες συμβαίνουν χωρίς να τις πολυκαταλαβαίνει γύρω του.

Κάθε μια από τις επεξεργασίες αυτές πιθανώς ρυθμίζεται από το Δίκαιο Προστασίας Δεδομένων.

Η Ελλάδα επομένως πολύ γρήγορα (σαφώς γρηγορότερα από άλλα ευρωπαϊκά κράτη) μετέβη από την κατάσταση ανύπαρκτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε κατάσταση πλήρους και εντατικής τους εκμετάλλευσης. Το χτύπημα για τον μέχρι πρότινος ανυποψίαστο Έλληνα πολίτη είναι διπλό: ενώ στην αρχή ενδιαφέρον έδειχνε σχεδόν αποκλειστικά ο ιδιωτικός τομέας, η ελληνική Αστυνομία φαίνεται ότι σιγά σιγά έχει και αυτή αξιώσεις συμμετοχής στην Ψηφιακή Ελλάδα.

Ο ελληνικός ιδιωτικός τομέας έδειξε πρώτος ενδιαφέρον για τα δεδομένα προσωπικού χαρακτήρα των Ελλήνων. Αναπόφευκτα, αφού η σύγχρονη οικονομία στηρίζεται και στην κατά το δυνατό εκτεταμένη διαχείριση πληροφοριών, μια Οικονομία της Πληροφορίας για την «*Κοινωνία της Πληροφορίας*». Το πρώτο πεδίο που ο Έλληνας καταναλωτής ένιωσε την αλλαγή ήταν ο Τειρεσίας –ενώ τα πρώτα χρόνια λειτουργίας του σχεδόν κανείς δεν γνώριζε για την ύπαρξή του, σήμερα σχεδόν όλοι τον τρέμουν. Η ύπαρξη ενός συστήματος βαθμολόγησης δανειοληπτών (credit-scoring system) είναι αυτονόητα απαραίτητη για κάθε κράτος που αποφασίζει να κινηθεί σε (οικονομικό) περιβάλλον χαμηλών επιτοκίων και, συνακόλουθα, υψηλού δανεισμού. Η δυσχέρεια με την ελληνική πραγματικότητα είναι ότι μέσα σε 5-10 χρόνια και χωρίς κάποια ιδιαίτερη ενημέρωση και συζήτηση για το γεγονός κλήθηκε να ανταποκριθεί σε ό,τι άλλα κράτη, ιδίως οι αγγλοσάξονες, βίωναν για δεκαετίες.

Στη συνέχεια, η επεξεργασία δεδομένων βγήκε από το παρασκήνιο: εταιρείες άμεσου μάρκετινγκ (direct marketing), τηλεφωνικά κέντρα (call centers), αυτοματοποιημένες μηχανές αποστολής μαζικών μηνυμάτων (spammers) και πληθώρα άλλων επιχείρησαν, και επιχειρούν, να επικοινωνήσουν απευθείας με τους δυνητικούς καταναλωτές τους. Στην πορεία ανέκυψαν και παράνομες πωλήσεις σε τρίτους καταλόγων επαγγελματικών συλλόγων με δεδομένα των μελών τους (π.χ. Δικηγορικός Σύλλογος Αθηνών), ενώ θέμα χρόνου είναι πότε το ελληνικό Κράτος θα χάσει ηλεκτρονικά αποθηκευμένα δεδομένα πολιτών (όπως στο Ηνωμένο Βασίλειο) και θα το μάθουμε.

Ενώ λοιπόν ο ελληνικός ιδιωτικός τομέας έχει αναπτύξει υπερδεκαετή έντονη δραστηριότητα επεξεργασίας των δεδομένων του μέσου Έλληνα ο δημόσιος τομέας βράδυνε. Στην ουσία δηλαδή η Ελλάδα μπήκε στο παιχνίδι επεξεργασίας δεδομένων μόλις στη δεύτερη φάση του, έχασε δηλαδή τη δεκαετία του 1970 και ξεκίνησε τη δεκαετία του 1980 ή μάλλον στην αρχή του 1990, όταν αντίπαλος πλέον ήταν ο ιδιωτικός τομέας. Κατά τη δεύτερη αυτή φάση οι επεξεργασίες του ελληνικού Δημοσίου μάλλον περιορίστηκαν σε εκείνες, επαπειλούμενες ή πραγματικές, της Εφορίας. Η ελληνική Αστυνομία μέχρι το 2004 μάλλον δεν είχε αντιληφθεί ότι συντρέχει τάση για Ψηφιακή Ελλάδα.

Εν έτει όμως 2009 η Ελλάδα αναμένεται να γευτεί πλήρως την τρίτη ιστορική φάση του Δικαίου Προστασίας Δεδομένων, την αναγέννηση δηλαδή

του Κράτους ως αντιπάλου μέσω των επεξεργασιών, πλέον, της Αστυνομίας για σκοπούς καταστολής (ή, ακόμα χειρότερα, πρόληψης) –περισσότερα όμως γι' αυτό παρακάτω.

Ρόλο οδηγού και συντρόφου του πολίτη στον κακοτράχαλο αυτόν δρόμο έχει η Αρχή Προστασίας Δεδομένων. Σε αυτήν άλλωστε απένειμε ο βασικός νόμος για την επεξεργασία δεδομένων την αρμοδιότητα «*ελέγχου της εφαρμογής του στην Ελλάδα*».

Για το πώς ακριβώς οφείλει η Αρχή να το κάνει αυτό καθένας μπορεί να έχει διαφορετική άποψη. Η (ελληνική ή και οποιαδήποτε άλλη στον κόσμο) Αρχή Προστασίας Δεδομένων μπορεί να κάνει οτιδήποτε μεταξύ του να σταθεί επικοινωνιακά δίπλα στο άτομο μέχρι να καθίσει στον «γυάλινο πύργο» της και να νομοθετεί αφ' υψηλού τα υποκείμενά της. Η ελληνική Αρχή μάλλον αυτο-τοποθετήθηκε στο δεύτερο άκρο. Αυτή η εξέλιξη ίσως ήταν αναπόφευκτη εξαιτίας της, *δια νόμου*, δομής της.

Αποτίμηση του έργου της ελληνικής Αρχής Προστασίας Δεδομένων μέχρι σήμερα δεν μπορεί να γίνει βέβαια εδώ. Εδώ ενδιαφέρει η οπτική του μέσου Έλληνα και μόνο. Από αυτή την άποψη αποφάσισε να ξεκινήσει την καριέρα της μάλλον ανορθόδοξα. Επειδή ίσως κάποιος μπόλιασε την πρώτη Αρχή Προστασίας Δεδομένων με το γερμανικό παράδειγμα (όπου η προστασία δεδομένων έγινε γνωστή σε όλους τους πολίτες εν μία νυκτί με μια μεγάλη υπόθεση, εκείνη της γενικής απογραφής του πληθυσμού) και επειδή σαφώς κατά τα πρώτα χρόνια υπήρχαν προβλήματα αναγνωρισιμότητας (αν όχι και αποδοχής), επιλέχθηκε ο στόχος των αστυνομικών ταυτοτήτων. *Δια νόμου* λοιπόν, ή πάντως με κανονιστική απόφαση της Αρχής Προστασίας Δεδομένων, διεγράφη το θρήσκευμα από τις αστυνομικές μας ταυτότητες. Για την περίπτωση αυτή επιλέχθηκε δηλαδή σίγουρος στόχος: πράγματι, χωρίς καμία αμφιβολία σε προηγμένο δυτικού τύπου Κράτος με νόμο Προστασίας Δεδομένων η αναγραφή του θρησκεύματος στις ταυτότητες (ή και οπουδήποτε αλλού, άλλωστε) είναι παράνομη. Ήταν όμως αυτή η επιλογή πράγματι σκόπιμη κατά το χρόνο στον οποίον έγινε; Η συνέχεια είναι γνωστή σε όλους. Η Ελλάδα διχάστηκε, στις εκκλησίες έγιναν «δημοψηφίσματα», τελικά η Αρχή Προστασίας Δεδομένων αποξένωσε τον μόνο τον οποίον ήθελε να φέρει κοντά της, δηλαδή τον (απλό) μέσο Έλληνα, που πιθανώς δεν έχει τα μέσα να αντιληφθεί και να προστατευτεί στην «*Κοινωνία της Πληροφορίας*» που μέσα σε λίγα χρόνια τον κάλυψε.

Αφού τέλος πάντων έγινε γνωστή, η Αρχή Προστασίας Δεδομένων έμενε να δείξει αν εκλάμβανε τον ρόλο της ως κυρίως κανονιστικό ή κυρίως εκπαιδευτικό. Αν δηλαδή σκοπός της ήταν να ρυθμίσει τις ελληνικές επεξεργασίες δεδομένων ή να βοηθήσει τον μέσο Έλληνα να προστατευτεί από αυτές με δικά του μέσα όσο καλύτερα γίνεται. Σειρά ενεργειών της έδειξε ότι ο πρώτος

ρόλος της ήταν πιο ελκυστικός (ή πιο εύκολος). Η Αρχή Προστασίας Δεδομένων δηλαδή επενέβη επανειλημμένα και ρύθμισε, για παράδειγμα, τον Τύπο κάθε φορά που δεδομένα «επωνύμων» έβγαιναν στο φως, την Αστυνομία όταν πρωτο-αποφάσισε να τοποθετήσει CCTV κάμερες στους δρόμους, τις εταιρείες τηλεφωνίας ή και τις τράπεζες.

Αντίθετα η Αρχή Προστασίας Δεδομένων ουδέποτε εξέδωσε κώδικες δεοντολογίας ή διοργάνωσε επικοινωνιακή εκστρατεία για να ενημερώσει το άτομο π.χ. για τον Τειρεσία, για το Ίντερνετ, για τις κάρτες πιστότητας (loyalty cards) των σούπερ μάρκετ, ή, πιο πρόσφατα, για τη διατήρηση δεδομένων (data retention). Η προσέγγιση δηλαδή δεν είναι ανθρωποκεντρική, αλλά κανονιστική: η Αρχή Προστασίας Δεδομένων προτιμά να επιβάλλει πρόστιμα σε όποιον παραβαίνει διατάξεις νόμου παρά να ενημερώνει προληπτικά πολίτες και υπεύθυνους επεξεργασίας ώστε να μειωθεί ο αριθμός των θυμάτων των παραβάσεων αυτών.

Ο μέσος Έλληνας, επομένως, βοήθεια μπορεί να περιμένει από την Αρχή μόνο κατασταλτικά, αν τυχόν αντιληφθεί παράνομη χρήση των δεδομένων του και μπορέσει να εντοπίσει την πηγή. Μέχρι το σημείο εκείνο πρέπει να βοηθήσει ο ίδιος τον εαυτό του.

Δυο είναι οι πηγές προβλημάτων για τον μέσο Έλληνα όσον αφορά την επεξεργασία δεδομένων του. Η πρώτη είναι οι *δια νόμου* επιβαλλόμενες επεξεργασίες που επιβάλλουν οι οπαδοί της θεωρίας του Μεγάλου Αδελφού. Η δεύτερη είναι οι νέες στρατηγικές πωλήσεων που εκπονούν ευρηματικοί μαρκετίστες.

Όσον αφορά τις *δια νόμου* επιβαλλόμενες επεξεργασίες, αυτές αφορούν μια κατηγορία επεξεργασιών που θα απασχολήσει πολύ στο μέλλον. Όπως θα αναλυθεί αμέσως παρακάτω, μετά την 11/9 το Δίκαιο Προστασίας Δεδομένων δεν θα είναι ποτέ πια το ίδιο. Συνεχώς εκπονούνται νέοι νόμοι που επιτρέπουν την επεξεργασία δεδομένων για σκοπούς κρατικής ασφάλειας. Οι τομείς των τηλεπικοινωνιών (data retention) ή της μετακίνησης των πολιτών (δεδομένα επιβατών/PNR) είναι μόνο η αρχή ενός φαινομένου που αργά ή γρήγορα θα οδηγήσει εκ των πραγμάτων σε κοινωνία Μεγάλου Αδελφού. (Και να σκεφτεί κανείς ότι εμείς σε αυτή τη μεριά του Ατλαντικού θεωρούμαστε και υπερβολικά προστατευτικοί του ατόμου στο θέμα.)

Δια νόμου επεξεργασίες έχουμε όμως και σε «εσωτερικό» επίπεδο (υπενθυμίζεται ότι η Οδηγία ρυθμίζει μόνο τις εμπορικές επεξεργασίες, η Ευρωπαϊκή Επιτροπή που την εξέδωσε δεν έχει δικαίωμα να νομοθετεί για θέματα ασφαλείας). Κατά τα τέλη του 2007, μετά από καταστροφική αντιπαλότητα της Αστυνομίας με την Αρχή Προστασίας Δεδομένων, το Υπουργείο Δικαιοσύνης έκρινε σκόπιμο να περιορίσει το πεδίο εφαρμογής του βασικού νόμου για την επεξεργασία δεδομένων ώστε να εξαιρέσει το σύνολο σχεδόν των επεξερ-

γασιών της Αστυνομίας. Οι συνθήκες ήταν ίσως ώριμες, αφού η χώρα ήδη προβληματιζόταν για το αν στοιχεία παιδόφιλων πρέπει να παρέχονται on-line (ένας διάλογος που η ύπαρξή του και μόνο αφήνει περιθώρια αισιοδοξίας για την Ψηφιακή Ελλάδα) ενώ αναμένονταν και τα πατροπαράδοτα επεισόδια κατά την πορεία για την επέτειο του Πολυτεχνείου.

Ο μέσος Έλληνας λοιπόν, και αν ακόμα υποτεθεί ότι είναι θετικός να δημοσιεύονται στο Διαδίκτυο τα στοιχεία των παιδόφιλων και να μην καίγεται κάθε χρόνο το κέντρο της Αθήνας, κατέληξε με πολύ περισσότερα από όσα ζήτησε: ξαφνικά *δια νόμου* το σύνολο των επεξεργασιών της Αστυνομίας εξαιρέθηκε από την εφαρμογή του Δικαίου Προστασίας Δεδομένων, μια σαφής χειροτέρευση του επιπέδου προστασίας ατομικών δικαιωμάτων στη χώρα.

Η δεύτερη πηγή προβλημάτων για τον μέσο Έλληνα είναι η αγορά. Σε περιόδους κρίσης και συνακόλουθης ανάγκης να συμπιεστούν οι δαπάνες, οι επιχειρήσεις αυτονόητα επιζητούν να γνωρίσουν τους πελάτες τους καλύτερα. Οποιαδήποτε όμως «προσωποποίηση» υπηρεσιών στηρίζεται σε επεξεργασία δεδομένων. Κάθε φορά που μας αναγνωρίζει στο τηλέφωνο ή δια ζώσης οποιοσδήποτε, από την πιτσαρία στη γειτονιά μας μέχρι τον προσωπικό μας τραπεζίτη (private banking) ή τον χρηματιστή μας, όλοι αυτοί μπροστά τους έχουν τα πλήρη στοιχεία μας. Ομοίως, κάθε φορά που χρησιμοποιούμε το Διαδίκτυο, στοιχεία μας συλλέγουν όλοι, από τον πάροχο πρόσβασης/ISP, που σύντομα θα υποχρεωθεί να τα παρέχει on-line στην Αστυνομία στο πλαίσιο της διατήρησης δεδομένων (data retention), μέχρι το εκάστοτε μέσο κοινωνικής δικτύωσης (social network) όπου έχουμε φτιάξει τους προσωπικούς μας δικτυακούς τόπους ή το ηλεκτρονικό κατάστημα Amazon από όπου αγοράζουμε τα βιβλία μας και που υπομονετικά μας περιμένει όποτε το ξαναεπισκεπτόμαστε με νέες προτάσεις για αγορές.

Χωρίς υπερβολή, οποιαδήποτε νέα υπηρεσία, οποιαδήποτε προσφορά ή οποιαδήποτε αγοραπωλησία σήμερα πραγματοποιείται στον πραγματικό ή στον on-line κόσμο εντός ή εκτός Ελλάδας περιλαμβάνει ανταλλαγή δεδομένων προσωπικού χαρακτήρα. Αυτό είναι μια γνώση που πρέπει να έχει πάντα στο πίσω μέρος του μυαλού του ο μέσος Έλληνας, χρήστης ή μη νέων τεχνολογιών.

Βασικό ζητούμενο επομένως σήμερα για τον μέσο Έλληνα είναι η αυτοπροστασία του, όσον αφορά την επεξεργασία των δεδομένων του. Σε περιβάλλοντα συνεχώς μεταβαλλόμενα, είτε *δια νόμου* είτε μέσω της αγοράς, η Αρχή Προστασίας Δεδομένων δεν μπορεί (και δεν είναι δυνατό ποτέ να μπορέσει) να ρυθμίσει κάθε επεξεργασία εκ των προτέρων. Καταφυγή επομένως σε αυτήν θα γίνεται όταν πλέον η ζημιά θα έχει γίνει.

Δυστυχώς στην προσπάθεια αυτοπροστασίας του ο μέσος Έλληνας έχει αφεθεί απελπιστικά μόνος. Κανείς δεν ασχολείται μαζί του, να τον ενημερώ-

Ψηφιακη Ελλαδα

ιστορική διαδρομή, σύγχρονο ρυθμιστικό πλαίσιο, προτάσεις για το μέλλον

Με δεδομένο ότι η επίτευξη της Ψηφιακής Ελλάδας είναι νομοτελειακή, αναρωτιέται κανείς αν εφαρμόζεται κάποιο σχέδιο για το πώς θα φτάσουμε εκεί, ή αν βαδίζουμε στα τυφλά παρασυρόμενοι από τις εξελίξεις. Οι πρωτοβουλίες και οι αριθμοί είναι εντυπωσιακοί: το ελληνικό Δημόσιο έχει δαπανήσει κατά την τελευταία δεκαετία δισεκατομμύρια ευρώ σε δράσεις που σχετίζονται με τη μετατροπή της χώρας σε τεχνολογικά ανεπτυγμένο κράτος, και μάλιστα στην on-line μορφή του. Το πλήθος των ελληνικών νοικοκυριών με συνδέσεις Internet, ευρυζωνικές ή μη, αυξάνεται με ραγδαίους ρυθμούς. Οι ελληνικές επιχειρήσεις είναι πλέον αδιανόητο να μη διαθέτουν πρόσβαση στο Internet — αν μη τι άλλο, για να διεκπεραιώνουν τις φορολογικές, ασφαλιστικές, και τραπεζικές εργασίες τους. Καθημερινά, καθένας από μας λαμβάνει δεκάδες προσκλήσεις από Διαδικτυακούς τόπους κοινωνικής δικτύωσης (social networks). Μπορεί οι αριθμοί διείσδυσης να κρίνονται ακόμα μη ικανοποιητικοί, αλλά είναι γεγονός ότι η ηλεκτρονική παρουσία (η ψηφιακή persona) έχει γίνει πλέον επαγγελματικό και προσωπικό μέλημα κάθε φυσικού και νομικού προσώπου στη χώρα.

Ο στόχος αυτού του βιβλίου είναι διπλός: αφενός να καταγράψει και αφετέρου να προτείνει. Η καταγραφή αφορά την Ψηφιακή Ελλάδα σήμερα, την ιστορική της διαδρομή και το σύγχρονο ρυθμιστικό πλαίσιο. Οι προτάσεις αφορούν την πορεία της στο μέλλον. Η αφετηρία της ανάλυσης είναι νομική, με την έννοια ότι η ανάλυση του ρυθμιστικού πλαισίου στους επιμέρους τομείς της Ψηφιακής Ελλάδας αποτελεί τον πυρήνα της. Στόχος της όμως δεν είναι να δοθούν νομικές απαντήσεις, αλλά να καταδειχθεί η σχέση μεταξύ νόμων και Ψηφιακής Ελλάδας. Με άλλα λόγια, η ανάλυση που γίνεται στο βιβλίο επιχειρεί να απαντήσει στα ερωτήματα: πώς δημιουργήθηκε το ισχύον νομικό πλαίσιο για τις νέες τεχνολογίες στη χώρα, πόσο αποτελεσματικά λειτουργεί στην πράξη, και πώς θα μπορούσαμε να κινηθούμε ασφαλέστερα και αποτελεσματικότερα προς μια πραγματική Ψηφιακή Ελλάδα στο — όχι και τόσο μακρινό — μέλλον.

Ο συγγραφέας

Ο **Βαγγέλης Παπακωνσταντίνου** είναι δικηγόρος, Διδάκτωρ Νομικής του Πανεπιστημίου Γκαίτε της Φρανκφούρτης. Περισσότερα στοιχεία γι' αυτόν μπορεί να βρει κανείς στη σελίδα *www.pkpartners.gr/vpapakonstantinou.html*.

εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ
Δαμοκοί 4, Σταθμός Λαρίσης, 10440 ΑΘΗΝΑ, Τηλ. 210-5287605
Επισκεφθείτε μας στο Internet:
www.klidarithmos.gr

ISBN 978-960-461-381-6