

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ ΔΙΟΙΚΗΣΗ

ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**ΘΕΜΑ: ΔΗΜΟΣΙΕΥΣΗ ΣΤΟΙΧΕΙΩΝ ΤΡΙΤΩΝ ΣΤΟ
ΔΙΑΔΙΚΤΥΟ. Η ΔΙΕΘΝΗΣ ΔΙΑΣΤΑΣΗ**

**THEISIS: PERSONAL DATA PUBLICATION OF PEOPLE
ON THE INTERNET. THE INTERNATIONAL
DIMENSION**

ΕΠΙΜΕΛΕΙΑ: ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ ΦΩΤΙΟΣ

ΛΙΑΕΣ ΙΩΑΝΝΗΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΠΑΧΟΥΡΟΣ ΑΝΤΩΝΙΟΣ

ΑΜΑΛΙΑΔΑ 2013

ΠΕΡΙΕΧΟΜΕΝΑ

<u>ΠΕΡΙΛΗΨΗ</u>	1
<u>ABSTRACT</u>	2
<u>ΕΙΣΑΓΩΓΗ</u>	3
<u>ΚΕΦΑΛΑΙΟ1: ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ</u>	
<u>1.1: Ιδιωτική ζωή</u>	5
<u>1.2: Προσωπικά Δεδομένα</u>	7
<u>1.2.1: Ιστορική επισκόπηση διεθνούς και κοινοτικής νομοθεσίας</u>	8
<u>1.2.2: Διάκριση των προσωπικών δεδομένων σε απλά και ευαίσθητα</u>	10
<u>1.2.3: Κατευθυντήριες αρχές επεξεργασίας προσωπικών δεδομένων</u>	11
<u>1.2.4: Δικαιώματα του υποκειμένου των δεδομένων</u>	13
<u>1.2.4.1: Το δικαίωμα της ενημέρωσης</u>	13
<u>1.2.4.2: Το δικαίωμα πρόσβασης</u>	14
<u>1.2.4.3: Το δικαίωμα αντίρρησης ή διόρθωσης</u>	15
<u>1.2.4.4: Το δικαίωμα προσωρινής δικαστικής προστασίας</u>	16
<u>ΚΕΦΑΛΑΙΟ 2: ΤΟ ΕΛΛΗΝΙΚΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ</u>	
<u>2.1: Η συνταγματική κατοχύρωση της προστασίας προσωπικών δεδομένων</u>	17
<u>2.2: Ο νόμος 2472/1997</u>	20
<u>2.2.1: Βασικές έννοιες του Ν.2472/1997</u>	21
<u>2.2.2: Επεξεργασία δεδομένων</u>	24
<u>2.3: Ο νόμος 3471/2006</u>	29

<u>2.3.1: Βασικές έννοιες του νόμου 3471/2006</u>	30
<u>2.3.2: Επεξεργασία δεδομένων</u>	32
<u>2.4: Πεδίο εφαρμογής του Ν.2472/1997 και Ν.3471/20063</u>	34

ΚΕΦΑΛΑΙΟ 3:ΤΟ ΔΙΕΘΝΕΣ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

<u>3.1: Η.Π.Α</u>	39
<u>3.1.1: Το σύνταγμα των Η.Π.Α</u>	40
<u>3.1.2: Ο νόμος για την ιδιωτική ζωή Privacy Act</u>	41
<u>3.1.3: Νόμοι των Η.Π.Α. σε σχέση με την προστασία προσωπικών δεδομένων</u>	46
<u>3.1.4: Αυτορύθμιση σε δημόσιο και ιδιωτικό τομέα</u>	48
<u>3.1.5: Διευθέτηση <<ασφαλούς λιμένα >> (safe harbor)</u>	51
<u>3.2: Γερμανία</u>	53
<u>3.2.1: Το Σύνταγμα, της Γερμανίας (Grundgesetz)</u>	54
<u>3.2.2: Ο Ομοσπονδιακός νόμος περί προστασίας προσωπικών δεδομένων (Bundesdatenschutzgesetz ή BDSG)</u>	56
<u>3.3: Γαλλία</u>	60
<u>3.3.1: Ο Νόμος Νο 78-17 της 6ης Ιανουαρίου 1978 επί της Informatique</u>	61
<u>3.3.2: Υποθέσεις χρήσης προσωπικών δεδομένων</u>	63
<u>3.4: Ηνωμένο Βασίλειο</u>	66
<u>3.4.1: Ο Data Protection Act 1998</u>	67
<u>3.4.2: Ο Freedom of Information Act 2000</u>	71
<u>3.5: Καναδάς</u>	73
<u>3.5.1: Ο Privacy Act του 1983</u>	74

<u>3.5.2: Ο νόμος για την Προστασία Προσωπικών Πληροφοριών και ηλεκτρονικών εγγράφων (P.I.P.E.D.A.)</u>	76
<u>3.6 Αυστραλία</u>	80
<u>3.6.1 Ο Privacy act 1988</u>	82
<u>3.7: Ιταλία</u>	90
<u>3.7.1: Ο νόμος no 196 του 2003</u>	91
<u>3.8: Κύπρος</u>	95
<u>3.8.1: Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα Νόμος 138(I) του 2001 με τις τροποποιήσεις του, 37(I) του 2003 και 105(I) του 2012</u>	96
<u>3.8.2: Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, 112(I)/2004 με τις τροποποιήσεις του, Νόμος 51(I) του 2012</u>	101
<u>ΕΠΙΛΟΓΟΣ-ΣΥΜΠΕΡΑΣΜΑΤΑ</u>	104
<u>ΒΙΒΛΙΟΓΡΑΦΙΑ</u>	108

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία έχει ως σκοπό την παρουσίαση και ανάλυση του θεσμικού πλαισίου που διέπει την δημοσίευση προσωπικών δεδομένων στο διαδίκτυο, σε διεθνές επίπεδο. Στο πρώτο κεφάλαιο αναλύονται οι όροι ιδιωτική ζωή και προσωπικά δεδομένα. Γίνεται διάκριση των απλών προσωπικών δεδομένων από τα ευαίσθητα και αναφέρονται οι κατευθυντήριες Αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων. Στο δεύτερο κεφάλαιο παρουσιάζεται το ελληνικό νομικό πλαίσιο προστασίας προσωπικών δεδομένων. Γίνεται αναφορά στο Ελληνικό Σύνταγμα και στους νόμους 2472/1997 και 3471/2006. Στο τρίτο κεφάλαιο παρουσιάζονται οι νομοθεσίες που διέπουν την προστασία προσωπικών δεδομένων επιλεγμένων χωρών. Αναφέρονται πρακτικές που ακολουθούν οι χώρες, πρωτοβουλίες για την ασφάλεια των δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων, οι υποχρεώσεις των ατόμων που διενεργούν την επεξεργασία, όπως επίσης και των παρόχων δικτύων τηλεπικοινωνιών. Στο τέταρτο κεφάλαιο ακολουθούν κάποια ουσιώδη συμπεράσματα που αφορούν την προστασία των προσωπικών δεδομένων, αναλύοντας τα μοντέλα προστασίας που χρησιμοποιούνται από κάθε χώρα.

Στην παρούσα εργασία ακολουθήθηκε η μεθοδολογία της έρευνας σε πρωτογενής πηγές, κυρίως σε διαδικτυακούς τόπους διεθνών οργανισμών και Αρχών προστασίας προσωπικών δεδομένων των χωρών που αναφέρονται. Χρησιμοποιηθήκαν βιβλιογραφικές πηγές, καθώς και επιστημονικά άρθρα που δημοσιεύθηκαν στον ημερήσιο Τύπο.

Στο σημείο αυτό θα θέλαμε να ευχαριστήσουμε των επιβλέπων καθηγητή μας Κ. Μπαχούρο Αντώνιο για τη βοήθεια που μας παρείχε, τη βιβλιοθήκη του δικηγορικού συλλόγου Λάρισας και τη βιβλιοθήκη του τμήματος της Νομικής του Αριστοτέλειου Πανεπιστημίου Θεσσαλονίκης για την πρόσβαση στις πηγές που μας παρείχαν.

ABSTRACT

This thesis purports to the presentation and analysis of the institutional framework, which governs the publication of personal data on the Internet, at an international level. In the first chapter, terms 'private life' and 'personal data', are analyzed. There is a discrimination between simple and sensitive personal data and the directional principles which govern the process of personal data are mentioned. In the second chapter, the Greek legal framework for protection of personal data is presented. There is a reference to the Greek constitution as well as to laws 2472/1997 and 3471/2006. In the third chapter, are presented the legislations that govern the protection of personal data in selected countries. Practices of countries, initiatives for security of data, rights of subjects over data, obligations of people who conduct the process as well as the provision of telecommunications network, are mentioned. In the fourth chapter, follow some essential conclusions over protection of personal data, analyzing the models of protection used by every country. This thesis was based on the methodology of research on primary sources, mainly on websites of international organizations and authorities for the protection of personal data of the countries mentioned. In addition, bibliographical sources as well as scientific articles, published in the daily press, were used. At this point, we would like to thank our supervising professor Mr. Bachouro Antonio, for providing assistance, the library of Larisa's Bar Association and the library of Law faculty at the Aristotelian university of Thessaloniki, for the access to all the information we were provided.

ΕΙΣΑΓΩΓΗ

Στην δεκαετία του 1970 έκανε την εμφάνιση της η ψηφιακή βιομηχανική επανάσταση, η οποία με την ανάπτυξη των δικτύων συντέλεσε στην απελευθέρωση της τηλεπικοινωνιακής αγοράς. Βασικό της χαρακτηριστικό είναι η δυνατότητα επικοινωνίας χωρίς όρια, χρονικά και εδαφικά. Τα τεχνικά εργαλεία εξελίσσονται διαρκώς και αντικαθίστανται από καινούργια, πιο γρήγορα και πιο μικρά σε διάσταση. Νέα λογισμικά, ανάπτυξη των δικτύων, συλλογή και επεξεργασία των πληροφοριών, χρήση διαδικτύου από τα κινητά, μικρές φορητές συσκευές μνήμης (usb), αποτελούν βασικά στοιχεία της νέας εποχής. Η ταχύτατη ανάπτυξη, διάδοση και χρήση των εφαρμογών της πληροφορικής προσφέρει τόσο σημαντικά πλεονεκτήματα, ώστε στις μέρες μας να μιλάμε για εξάρτηση του κράτους, των οικονομικών, της παιδείας και του πολιτισμού από την πληροφορική¹.

Η ραγδαία ανάπτυξη της τεχνολογίας της πληροφορικής και οι αυξημένες χάρη στην τεχνολογία δυνατότητες συλλογής, επεξεργασίας και ποικίλης χρήσης πληροφοριών, που αφορούν το άτομο, συνεπάγονται κινδύνους για επεμβάσεις στην ιδιωτική ζωή του ατόμου². Μέθοδοι και τεχνικές όπως τα cookies, το data warehouse (αποθήκη δεδομένων), το data mining (εξόρυξη δεδομένων), το sniffing software (λογισμικό-λαγωνικό), οι double agents (διπλοί πράκτορες), δυναμιτίζουν την εφαρμοσιμότητα των κανόνων για διαφανή, θεμιτή και νόμιμη συλλογή προσωπικών δεδομένων³. Τα προβλήματα προστασίας προσωπικών δεδομένων στο Internet είναι ιδιαίτερα σημαντικά, δεδομένου ότι διαπιστώνεται κυκλοφορία προσωπικών δεδομένων στο διαδίκτυο σε μεγάλη έκταση, αφού ακόμη και μια απλή περιήγηση στο διαδίκτυο

¹ Γρηγόρης Λάζος, Πληροφορική και έγκλημα, 2001, σελ. 16

² Ειρήνη Βασιλάκη, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, σελ. 1

³ Λίλιαν Μήτρου, Το δίκαιο στην κοινωνία της πληροφορίας, 2003, σελ. 35

δεν παραμένει ανώνυμη όσον αφορά το χρήστη. Έτσι ο κάθε χρήστης αδυνατεί να ελέγξει την ποσότητα και την ποιότητα των πληροφοριών που τον αφορούν, ενώ ταυτόχρονα δεν γνωρίζει τους αποδέκτες των πληροφοριών και τον σκοπό για τον οποίο χρησιμοποιούν τις πληροφορίες αυτές.

Η μετατροπή αυτή του χρήστη σε πηγή πληροφοριών⁴ δεν έχει μόνο οικονομική σημασία, αλλά και πολιτική. Η καταγραφή της ιδιωτικής ζωής του ατόμου οδηγεί και σε πληροφορίες που αφορούν τις πολιτικές του πεποιθήσεις και δραστηριότητες. Δίνεται με αυτό τον τρόπο η δυνατότητα να γίνει χρήση των προσωπικών του δεδομένων. Επίσης μία σειρά από εφαρμογές των ηλεκτρονικών επικοινωνιών το αποδεικνύουν. Ιστότοποι όπως το Facebook και το Twitter, χρησιμοποιούνται από εκατομμύρια χρήστες του διαδικτύου, εκθέτοντας στοιχεία, φωτογραφίες και video της προσωπικής τους ζωής, τα οποία μοιράζονται πολλές φορές με εκατοντάδες ή και χιλιάδες άτομα, στα οποία επιτρέπουν να έχουν πρόσβαση στα στοιχεία αυτά.

Μέσα σε αυτές τις συνθήκες είναι προφανής η ανάγκη για μία όσο το δυνατό μεγαλύτερη και πιο οργανωμένη προσπάθεια δημιουργίας νόμων, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, ώστε να ισορροπήσουν μεταξύ της ελεύθερης κυκλοφορίας των πληροφοριών και της προστασίας των χρηστών του διαδικτύου και των προσωπικών τους δεδομένων.

⁴ Μαντζούφα Π., Η διακινδύνευση στην κοινωνία της πληροφορίας και η προστασία των προσωπικών δεδομένων, 2007, σελ.1089

ΚΕΦΑΛΑΙΟ 1. ΙΔΙΩΤΙΚΗ ΖΩΗ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ [ΛΙΛΕΣ]

1.1 Ιδιωτική ζωή

Η ανάπτυξη των υπολογιστών και των δικτύων προκάλεσαν ένα ιδιαίτερο ενδιαφέρον για την προστασία της ιδιωτικής ζωής, για το λόγο αυτό υπάρχουν διάφορες προσεγγίσεις και διαφορετικές κανονιστικές ρυθμίσεις από χώρα σε χώρα, τόσο για την έννοια της ιδιωτικής ζωής, όσο και για τον τρόπο προστασίας της.

Στις Η.Π.Α. για ζητήματα προστασίας της ιδιωτικής ζωής χρησιμοποιείται ο όρος <<Privacy>> ή <<ιδιωτικότητα>>⁵ όπως μεταφράζεται. Η πίστη στην ελευθερία του ατόμου οδήγησε στην πεποίθηση ότι το κάθε άτομο είναι ελεύθερο να αποφασίσει αν οι πληροφορίες που το αφορούν μπορούν να γίνουν αντικείμενο καταγραφής ή επεξεργασίας, έτσι ο καθένας μπορεί να συναινέσει στη χρήση των πληροφοριών που τον αφορούν, ενώ ο εκτελών την επεξεργασία⁶ των πληροφοριών αυτών ευθύνεται για τη συμφωνημένη χρήση τους, δηλαδή για τη συγκατάθεση του υποκειμένου των δεδομένων⁷. Στην Ευρώπη, σε αντίθεση με τις ΗΠΑ, δόθηκε έμφαση στην προστασία της ιδιωτικής ζωής ώστε να μην θίγεται η αξιοπρέπεια του ατόμου και να μην προσβάλεται η υπόληψη και η προσωπικότητα του. Μια μεγάλη περίοδος απολυταρχικών καθεστώτων, όπου η ιδιωτική ζωή δεν τύγχανε ιδιαίτερου σεβασμού,

⁵ Μαυριά Κ., Τα ο συνταγματικό δικαίωμα του ιδιωτικού βίου, 1982, σελ.59

⁶ www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#2 (08/04/2013)

“Εκτελών την επεξεργασία”, οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

⁷ www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#2 (08/04/2013)

“Υποκείμενο των δεδομένων”, το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων

οδήγησε την Ευρωπαϊκή Ένωση να δώσει έμφαση στη ρύθμιση της προστασίας της ιδιωτικής ζωής,⁸ έτσι δημιουργήθηκαν συνθήκες για τη διασφάλιση αυτών των ελευθεριών με την εγγύηση του κράτους, όπου μέσα από αυστηρό νομοθετικό πλαίσιο, διασφαλίζει τις ελευθερίες των πολιτών και τους παρέχει το δικαίωμα προσφυγής σε δικαστήριο.

Μία βασική διαφορά της ευρωπαϊκής συνταγματικής προσέγγισης σε σχέση με την αντίστοιχη των ΗΠΑ, είναι ότι στις ΗΠΑ ένα άτομο μπορεί να επικαλεστεί την ιδιωτικότητα ως δικαίωμα μόνο έναντι του Κράτους, το οποίο δεν υποχρεούται σε παρέμβαση έναντι των ιδιωτών,⁹ ενώ το ευρωπαϊκό Δικαστήριο αναγνωρίζει αφενός την υποχρέωση του κράτους να λαμβάνει μέτρα για την προστασία των δικαιωμάτων των προσώπων στην ιδιωτικότητα, και αφετέρου την πιθανή ευθύνη του κράτους για παραβιάσεις της ιδιωτικότητας εκ μέρους ιδιωτών, εφόσον δεν έχει λάβει μέτρα για την αποτροπή ή την κύρωσή τους.

Η πιο γνωστή φράση που μπορεί να περιγράψει τον όρο ιδιωτική ζωή είναι: <<the right to be let alone>> η οποία διατυπώθηκε από τους Samuel Warren και Luis Brandeis, το 1980 στο άρθρο τους <<The right to privacy>>¹⁰, υποστηρίζοντας ότι το δικαίωμα του να μένει κανείς μόνος του αποτελεί το πιο θεμελιώδες δικαίωμα που επιθυμούν οι ελεύθεροι λαοί, καθώς το άτομο προσπαθεί να προστατευθεί από τον κοινωνικό έλεγχο και να διασφαλίσει την προσωπική του ταυτότητα και ελευθερία.

Σε άλλες περιοχές του κόσμου όμως το δικαίωμα στην ιδιωτική ζωή έχει διαφορετική διάσταση. Σε χώρες της Αφρικής, ο Αφρικανικός Χάρτης Ανθρωπίνων Δικαιωμάτων δίνει έμφαση στα κοινωνικά δικαιώματα, όπως οικογένεια, κράτος, κοινότητα, και δεν αναφέρει το δικαίωμα στην ιδιωτική ζωή¹¹, επίσης σε χώρες του

⁸ Cate F. Privacy and Telecommunications, 1998, σελ. 15

⁹ L. A. Bygrave, Privacy Protection in a Global Context – A Comparative Overview. Scandinavian Studies in Law, 2004, σελ. 319-348

¹⁰ Samuel Warren and Luis Brandeis, The right to privacy, Harvard Law Review, vol.IV, 1980, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (08/04/2013)

¹¹ Serge Gutwirth, Privacy and the information age, 2002, σελ.24

Ισλάμ ο άνθρωπος αντιμετωπίζεται ως μέλος μιας ομάδας, που πάνω από κάθε νομό πρέπει να ακολουθεί της επιταγές του Αλλάχ, έτσι η Οικουμενική Διακήρυξη Ανθρωπίνων Δικαιωμάτων είναι απλά ένας ανθρώπινος νόμος. Σε αντίθεση με την Ιαπωνία, όπου το άρθρο 13 του Ιαπωνικού Συντάγματος αναφέρει αδιαμφισβήτητα το δικαίωμα στη <<ζωή, ελευθερία και επιδίωξη της ευτυχίας>>¹².

Στην Ελλάδα η ιδιωτική ζωή ορίζεται ως <<ο χώρος που αυτοπροσδιορίζει κάθε άτομο προκειμένου να ασκεί μέσα σε αυτόν προσωπικές και οικογενειακές δραστηριότητες χωρίς παρενοχλήσεις τρίτων, ο χώρος αυτός εκτίνεται μεταξύ της κοινωνικής και επαγγελματικής ζωής και του χώρου της αυστηρά προσωπικής του ζωής>>¹³. Προστατεύεται από το Ελληνικό Σύνταγμα με τα άρθρα 9 και 9Α. Η συνταγματική διακήρυξη του απαραβίαστου της ιδιωτικής ζωής σημαίνει την απαγόρευση της δημοσιοποίησης της ζωής του ανθρώπου¹⁴.

1.2 Προσωπικά Δεδομένα

Όπως ήδη επισημάνθηκε, η αναγκαιότητά της προστασίας της ιδιωτικής ζωής περιλαμβάνει το δικαίωμα του ατόμου να ελέγχει τη συλλογή, τη χρήση και την αποκάλυψη των προσωπικών του δεδομένων. Συγκεκριμένα, βάση της Ευρωπαϊκής οδηγίας 95/46/EK (άρθρο 2 α), ως “δεδομένα προσωπικού χαρακτήρα” προσδιορίζονται <<όλες οι πληροφορίες που αφορούν ένα φυσικό πρόσωπο, του οποίου ή ταυτότητα είναι γνωστή ή μπορεί να προσδιοριστεί άμεσα ή έμμεσα ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν

¹² Serge Gutwirth, *Privacy and the information age*, 2002,σελ.2

¹³ Καράκωστας Ι., *Προστασία της ιδιωτικότητας στην κοινωνία της Πληροφορίας*, 2004, σελ.56

¹⁴ Π.Δ. Δαγτόγλου, *Συνταγματικό Δίκαιο, Ατομικά και Κοινωνικά Δικαιώματα*, 2005, σελ.390

την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική>>.

Τα προσωπικά δεδομένα πρέπει να είναι πληροφορίες που ταυτίζονται με ένα συγκεκριμένο άτομο, δηλαδή πληροφορίες που χρησιμοποιούνται για να αναγνωριστεί ένα πρόσωπο και μπορούν να περιλαμβάνουν το όνομα, τη διεύθυνση, το τηλέφωνο, τη φυλή, την οικογενειακή κατάσταση, τον αριθμό κοινωνικής ασφάλισης, τον αριθμό πελάτη. Οι πληροφορίες αυτές μπορούν να αφορούν ακόμη και σχέσεις ενός ατόμου με άλλα άτομα ή ακόμα και σχέσεις ενός ατόμου με το περιβάλλον, όπως δραστηριότητες, συνήθειες, τρόπος ζωής, και καταναλωτική συμπεριφορά.

1.2.1.Ιστορική επισκόπηση διεθνούς και κοινοτικής νομοθεσίας

Το γερμανικό κρατίδιο της Έσσης το 1970 ήταν το πρώτο που προσπάθησε να ρυθμίσει το ζήτημα της προστασίας των προσωπικών δεδομένων (Hesse data protection act). Ακολούθησαν η Αυστρία, η Γαλλία, η Γερμανία, και στη συνέχεια όλες οι Ευρωπαϊκές χώρες. Την ίδια περίοδο ψηφίστηκε στις ΗΠΑ ο νόμος Privacy Act του 1974.

Το πρώτο διεθνές νομικά δεσμευτικό κείμενο για την προστασία των προσωπικών δεδομένων είναι η σύμβαση του Στρασβούργου ή σύμβαση 108 το 1981 "Για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα". Επιχειρεί τη διασφάλιση τόσο του ιδιωτικού βίου, όσο και της ελεύθερης κυκλοφορίας των πληροφοριών από τη μία χώρα στην άλλη. Είναι η πρώτη φορά που σε συλλογικό επίπεδο τεθήκαν οι όροι και οι κανόνες για τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα.¹⁵ Η σύμβαση τέθηκε σε ισχύ

¹⁵ Κυριακόπουλος Γ., Ασφάλεια και επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Οι ρυθμίσεις του Συμβουλίου της Ευρώπης, ΔτΑ 11/2001, σελ. 763

την 1^η Οκτωβρίου του 1985. Ένα ακόμη σημαντικό νομοθετικό κείμενο το 1989 ήταν η Διακήρυξη των Θεμελιωδών Δικαιωμάτων και Ελευθεριών. Το 1990 η Γενική Συνέλευση του Ο.Η.Ε. ενέκρινε τις "Κατευθυντήριες Αρχές Προστασίας Προσωπικών Δεδομένων σε αυτοματοποιημένα αρχεία", που συνέταξε η Επιτροπή των Δικαιωμάτων του Ανθρώπου του Ευρωπαϊκού Κοινοβουλίου. Θεμελιώδες νομοθετικό κείμενο για την προστασία των προσωπικών δεδομένων υπήρξε η Οδηγία 95/46/EK "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα". Η Οδηγία 95/46/EK του Ευρωπαϊκού Κοινοβουλίου έχει ως στόχο την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής του ατόμου, και την εξασφάλιση της ελεύθερης κυκλοφορίας των προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Στη συνέχεια, η οδηγία 2002/58/EK η οποία αναθεωρεί την Οδηγία 97/96/EK, επιβάλλει τη θέσπιση ειδικών νομικών και τεχνικών διατάξεων για την προστασία βασικών δικαιωμάτων και ελευθεριών. Η δυνατότητα προστασίας των δεδομένων προσωπικού χαρακτήρα των χρηστών αποτελεί προϋπόθεση για την ανάπτυξη του ηλεκτρονικού εμπορίου. Με την Οδηγία 2002/58/EK εναρμονίζονται οι διατάξεις των κρατών μελών, οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών και των εξοπλισμών και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ευρωπαϊκή Ένωση.

Στην Ελλάδα η κοινοτική οδηγία 95/46/EK ενσωματώνεται με το Νόμο 2472/97, ο οποίος αναφέρεται στην "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα". Αντικείμενο του νόμου είναι η θέσπιση των προϋποθέσεων για τη επεξεργασία δεδομένων προσωπικού χαρακτήρα, για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων, και ιδίως της ιδιωτικής ζωής.

1.2.2 Διάκριση των προσωπικών δεδομένων σε απλά και ευαίσθητα

Τα προσωπικά δεδομένα δε διαθέτουν όλα την ίδια πληροφοριακή αξία, κάποια από αυτά παρουσιάζουν ένα βαθμό ευαισθησίας και διαφοροποιούνται από τα απλά προσωπικά δεδομένα, χρίζοντας ιδιαίτερης και αυστηρότερης προστασίας.

Ενδεικτικά, ως απλά προσωπικά δεδομένα μπορούμε να πούμε ότι είναι τα στοιχεία αναγνώρισης (στοιχεία ταυτότητας και καταγωγής), τα προσωπικά χαρακτηριστικά (φυσικά χαρακτηριστικά ,συνήθειες, προσωπικότητα), οι οικογενειακές συνθήκες (έγγαμος-άγαμος), η εκπαίδευση, η οικονομική κατάσταση και η εργασία.

Δεδομένου ότι δεν υπάρχει κάποια συγκεκριμένη αρχή, ή κριτήριο που να διαχωρίζει τα προσωπικά δεδομένα σε απλά και ευαίσθητα, απαριθμούμε ορισμένες κατηγορίες ευαίσθητων προσωπικών δεδομένων σύμφωνα με την Ευρωπαϊκή οδηγία 95/46/EK, αλλά και τον Εθνικό Νόμο 2472/1997 ο οποίος υιοθέτησε της κατηγορίες προσωπικών δεδομένων της οδηγίας προσθέτοντας κάποιες ακόμη. Ο Νόμος 2472/1997 ορίζει ως ευαίσθητα προσωπικά δεδομένα¹⁶:

- Τη φυλετική προέλευση
- Τα πολιτικά φρονήματα
- Τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- Τη συμμετοχή σε συνδικαλιστική οργάνωση, ένωση ή σωματείο
- Την κοινωνική πρόνοια
- Την υγεία
- Την ερωτική ζωή

¹⁶ www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#2 (08/04/2013)

- Δεδομένα που αφορούν καταδίκες η ποινικές διώξεις
- Τα γενετικά δεδομένα
- Τη συμμετοχή σε ενώσεις που σχετίζονται με ευαίσθητα προσωπικά δεδομένα¹⁷

1.2.3 Κατευθυντήριες αρχές επεξεργασίας προσωπικών δεδομένων.

Τα ποιοτικά χαρακτηριστικά των προσωπικών δεδομένων, απλών ή ευαίσθητων, είναι εκείνα που καθιστούν αποδεκτή την επεξεργασία τους. Ο Οργανισμός Οικουμενικής Συνεργασίας και Ανάπτυξης το 1980 έκδωσε τις <<Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυννοριακές ροές προσωπικών δεδομένων>>. ¹⁸ Οι αρχές αυτές δεν έχουν δεσμευτικό χαρακτήρα αλλά χρησιμοποιηθήκαν από πολλά κράτη που στερούνταν κάποιου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων, και αποτελούν τον πυρήνα των περισσότερων νόμων που αφορούν την προστασία προσωπικών δεδομένων.

- **Αρχή της ποιότητας των δεδομένων:** Αναφέρει ότι τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν, όπως επίσης, να είναι πλήρη, ακριβή και ενημερωμένα.
- **Αρχή του περιορισμού της συλλογής:** Αναφέρει ότι η συλλογή προσωπικών δεδομένων θα πρέπει να πραγματοποιείται θεμιτά και σύμφωνα με το νόμο, θα πρέπει να υπάρχει όριο στη συλλογή προσωπικών δεδομένων και όπου είναι δυνατό να γίνεται με την ενημέρωση και συγκατάθεση του χρήστη.

¹⁷ Αλεξανδροπούλου - Αιγυπτιάδου Ε., Προσωπικά Δεδομένα, 2007, σελ.34-37

¹⁸ Σωτηρόπουλο Β., Η συνταγματική προστασία των προσωπικών δεδομένων, 2006, σελ.15

- **Αρχή του περιορισμού της χρήσης:** Αναφέρει ότι τα προσωπικά δεδομένα δεν θα πρέπει να κοινοποιούνται σε τρίτους, ή να χρησιμοποιούνται για άλλο σκοπό από αυτόν για τον οποίο αποκτήθηκαν.
- **Αρχή του προσδιορισμού του σκοπού:** Αναφέρει ότι ο σκοπός για τον οποίο τα προσωπικά δεδομένα συλλέγονται θα πρέπει να προσδιορίζεται το αργότερο κατά τη στιγμή της συλλογής τους.
- **Αρχή της προστασίας της ασφάλειας:** Αναφέρει ότι τα προσωπικά δεδομένα θα πρέπει να προστατεύονται απέναντι σε κινδύνους, όπως η πρόσβαση, η χρήση, η τροποποίηση, και η κοινοποίηση σε τρίτους.
- **Αρχή της διαφάνειας:** Αναφέρει ότι θα πρέπει να υπάρχει μια διαφάνεια αναφορικά με τις πολιτικές και πρακτικές που χρησιμοποιούνται για τη συλλογή των δεδομένων, καθώς και για την ταυτότητα του φορέα που διενεργεί τη συλλογή.
- **Αρχή της συμμετοχής του ατόμου:** Αναφέρει ότι το κάθε άτομο έχει δικαίωμα να αποκτά επιβεβαίωση σχετικά με το αν ο υπεύθυνος επεξεργασίας έχει δεδομένα που το αφορούν, να του ανακοινώνονται δεδομένα που σχετίζονται με αυτόν σε εύλογο χρονικό διάστημα, να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του, που αναφέρονται στις δύο παραπάνω παραγράφους, και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης, της απόρριψης, και της περαιτέρω διεκδίκησης, ώστε να μπορεί να προχωρεί σε εξάλειψη, διόρθωση, ή ολοκλήρωση των δεδομένων αυτών.
- **Αρχή της ευθύνης:** Αναφέρει ότι ο κάθε υπεύθυνος της επεξεργασίας θα πρέπει να είναι υπόλογος για την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές.¹⁹

¹⁹ www.oecd.org/sti/interneteconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2 (08/04/2013)

1.2.4 Δικαιώματα του υποκειμένου των δεδομένων

Η διασφάλιση της διαύγειας και της σύννομης επεξεργασίας, εκδηλώνεται με την κατοχύρωση ενός συστήματος δικαιωμάτων του υποκειμένου των δεδομένων. Ο νόμος θεσπίζει τέσσερα θεμελιώδη δικαιώματα, τα οποία είναι: το δικαίωμα της ενημέρωσης, β) το δικαίωμα της πρόσβασης, γ) το δικαίωμα της αντίρρησης ή διόρθωσης και δ) το δικαίωμα δικαστικής προστασίας.

1.2.4.1. Το δικαίωμα της ενημέρωσης

Το δικαίωμα της ενημέρωσης προστατεύεται αυτοτελώς και αποτελεί βασική προϋπόθεση για την άσκηση των δικαιωμάτων της πρόσβασης και της αντίρρησης.²⁰ Κατοχυρώνει το δικαίωμα της πληροφοριακής αυτοδιάθεσης του ατόμου, σύμφωνα με το οποίο το υποκείμενο των δεδομένων πρέπει να γνωρίζει ποιος και για ποιο λόγο κάνει συλλογή ή επεξεργασία δεδομένων που τον αφορούν.²¹ Το υποκείμενο των δεδομένων έχει δικαίωμα ενημέρωσης ακόμη και όταν η επεξεργασία των δεδομένων του επιτρέπεται χωρίς τη συγκατάθεση του. Στο περιεχόμενο της ενημέρωσης πρέπει να αναφέρονται, σύμφωνα με το άρθρο 11 του νόμου 2472/1997, τα στοιχεία της ταυτότητας του φορέα επεξεργασίας όπως και του εκπροσώπου του, ο σκοπός της επεξεργασίας, οι αποδεκτές των δεδομένων και ενημέρωση για το δικαίωμα της πρόσβασης,²² όπως επίσης και ενημέρωση για κάθε μεταβολή των στοιχείων αυτών.

²⁰ Αλεξανδροπούλου - Αιγυπτιάδου Ε., Ζητήματα από το δίκαιο Πληροφορικής, 2002, σελ. 38

²¹ Γέροντα Α., Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, 2002, σελ.221

²² www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#11 (08/04/2013)

Όταν η συλλογή γίνεται με την συμβολή του υποκειμένου, η ενημέρωση πρέπει να γίνεται κατά το χρόνο της συλλογής των δεδομένων και εγγράφως, ενώ στην περίπτωση που η συλλογή γίνεται από άλλες πηγές, η ενημέρωση πρέπει να γίνει πριν από οποιαδήποτε χρήση ή επεξεργασία των δεδομένων αυτών,²³ με τρόπο πρόσφορο ώστε να εξασφαλίζεται η επαρκής πληροφόρηση του υποκειμένου. Για παράδειγμα, με μια μεγάλη πινακίδα στο χώρο συναλλαγής, ή αν πρόκειται για το διαδίκτυο με μια ευδιάκριτη επισήμανση στην αρχική σελίδα της ιστοσελίδας.

Άρση της υποχρέωσης ενημέρωσης του υποκειμένου των δεδομένων μπορεί να γίνει όταν η επεξεργασία γίνεται για λόγους εθνικής ασφάλειας, ή για την εξακρίβωση σοβαρών εγκλημάτων, όπως επίσης και όταν η συλλογή γίνεται για αποκλειστικά δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα.²⁴

1.2.4.2. Το δικαίωμα πρόσβασης

Το δικαίωμα πρόσβασης προστατεύεται αυτοτελώς, καθώς θεσπίζει τον έλεγχο του υπεύθυνου της επεξεργασίας από το υποκείμενο και κατοχυρώνει το δικαίωμα της πληροφοριακής αυτοδιάθεσης του. Το υποκείμενο έχει το δικαίωμα να ζητά και να λαμβάνει χωρίς καθυστέρηση όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και τον τρόπο απόκτησης τους, τον σκοπό της επεξεργασίας και τους αποδέκτες των δεδομένων, την εξέλιξη της επεξεργασίας, και το χρόνο που μεσολάβησε από την τελευταία του ενημέρωση. Όταν η επεξεργασία είναι αυτοματοποιημένη ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο για τον τρόπο και τα κριτήρια του συστήματος που στηρίζει την επεξεργασία των δεδομένων.²⁵

²³ Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων ,ΔΕΕ 1999, σελ.579

²⁴ Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων ,ΔΕΕ 1999, σελ.580

²⁵ Π. Αρμαμέντος, Β. Σωτηρόπουλος, Ερμηνεία Ν.2472/1997, 2005, άρθ. 12, σελ.762

Το δικαίωμα πρόσβασης ασκείται με την υποβολή αίτησης στον υπεύθυνο επεξεργασίας, αν ο υπεύθυνος επεξεργασίας δεν απαντήσει, ή η απάντηση του δεν είναι ικανοποιητική, το υποκείμενο έχει δικαίωμα να προσφύγει στην Αρχή Προστασίας Προσωπικών Δεδομένων. Άρση του δικαιώματος πρόσβασης μπορεί να γίνει με απόφαση της Αρχής μετά από αίτηση του υπεύθυνου επεξεργασίας όταν η επεξεργασία γίνεται για λόγους εθνικής ασφάλειας, ή για λόγους εξακρίβωσης σοβαρών εγκλημάτων.

1.2.4.3. Το δικαίωμα αντίρρησης ή διόρθωσης

Το δικαίωμα της αντίρρησης του υποκειμένου έχει ως σκοπό να προστατέψει τα συμφέροντα του υποκειμένου και να διασφαλίσει τον έλεγχο για τη νόμιμη επεξεργασία των δεδομένων,²⁶ επίσης το υποκείμενο έχει το δικαίωμα της διόρθωσης,²⁷ προσωρινής μη χρήσης, δέσμευσης και διαγραφής. Οι αντιρρήσεις υποβάλλονται εγγράφως στον υπεύθυνο επεξεργασίας ο οποίος έχει την υποχρέωση να απαντήσει εντός 15 ημερών. Στην απάντηση του οφείλει να ενημερώσει το υποκείμενο με τρόπο κατανοητό για της ενέργειες στις οποίες προβεί, ή για τους λόγους που δεν ικανοποίησε το αίτημα, όταν αυτό συμβαίνει. Σε αυτή την περίπτωση ο υπεύθυνος της επεξεργασίας πρέπει να κοινοποιήσει την απάντηση και στην Αρχή.

²⁶ Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων, ΤοΣ 1999, σελ.21

²⁷ Αλεξανδροπούλου - Αιγυπτιάδου Ε., Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου , 2005, Αρμ59, σελ.137

1.2.4.4. Το δικαίωμα προσωρινής δικαστικής προστασίας

Σύμφωνα με το δικαίωμα προσωρινής δικαστικής προστασίας, ο καθένας έχει το δικαίωμα να ζητήσει από το αρμόδιο δικαστήριο την άμεση αναστολή ή την μη εφαρμογή απόφασης που τον θίγει και έχει παρθεί από διοικητική αρχή, νομικό πρόσωπο ιδιωτικού ή δημοσίου δικαίου, ή φυσικό πρόσωπο, αποκλειστικά με αυτοματοποιημένη επεξεργασία δεδομένων. Το δικαίωμα αυτό ασκείται όταν η επεξεργασία αφορά την αξιολόγηση της προσωπικότητας του, της οικονομικής φερεγγυότητας του, της αξιοπιστίας του και της εν γένει συμπεριφοράς του.²⁸

²⁸ Αλεξανδροπούλου – Αιγυπτιάδου Ε., Προσωπικά Δεδομένα, 2007, σελ.98

ΚΕΦΑΛΑΙΟ 2: ΤΟ ΕΛΛΗΝΙΚΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ [ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ]

2.1 Η συνταγματική κατοχύρωση της προστασίας προσωπικών δεδομένων

Κλασική - σχεδόν αυθόρμητη, αλλά οπωσδήποτε εξηγήσιμη υπήρξε η αναζήτηση του συνταγματικού θεμέλιου στην «προστασία του ιδιωτικού βίου» όπως αυτή διαγράφεται στο άρθρο 9 παρ. 1 του Συντάγματος 1975/1986/2001. Η συλλογή και επεξεργασία προσωπικών δεδομένων, η “κατόπτευση” της ζωής ενός ατόμου, η εκπόνηση βιοπορτραίτων έχει ως άμεση συνέπεια ότι αυτός που συλλέγει και επεξεργάζεται πληροφορίες μπορεί μέσω αυτών (των πληροφοριών) να επεμβαίνει δραστικά στη ζωή των άλλων.²⁹ Η προσωπικότητα καθίσταται προβλέψιμη, ένα μέρος της ατομικότητας (και όχι μόνο του ιδιωτικού βίου) και της ελευθερίας ίδιου προγραμματισμού και δράσης αναιρείται και το πρόσωπο γίνεται “αντικείμενο” των συμφερόντων και επιδιώξεων των άλλων. Το δικαίωμα στην αυτοκαθοριζόμενη ζωή αποτελεί βασική συνιστώσα του γενικού δικαιώματος της ανάπτυξης της προσωπικότητας. Το άρθρο 5 § 1Σ³⁰ προστατεύει το δικαίωμα ελεύθερης ανάπτυξης της προσωπικότητας. Το δικαίωμα αυτό περιλαμβάνει την εγγύηση της αυτόνομης απόφασης του ατόμου για τη δημόσια και ιδιωτική παρουσίαση και εικόνα του, αλλά και την ελευθερία προσδιορισμού των πληροφοριών που θα καθίστανται γνωστές στο περιβάλλον του.³¹

²⁹ www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-9a/ (08/04/2013)

³⁰ www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-5a/ (08/04/2013)

³¹ Β. Σωτηρόπουλος, Η πρόσβαση στη δημόσια πληροφορία και η προστασία προσωπικών δεδομένων, 2005, Digesta, σελ. 95.

Στα συνταγματικά ερείσματα της προστασίας προσωπικών δεδομένων συγκαταλεγόταν αναμφίβολα και η ρύθμιση του άρθρου 2 § 1 που αναγορεύει τον σεβασμό και την προστασία της αξίας του ανθρώπου σε πρωταρχική υποχρέωση της πολιτείας. Η αξιοπρέπεια που ξεχωρίζει τον άνθρωπο είναι ακριβώς η ελευθερία του, νοούμενη μεταξύ άλλων ως ελευθερία επιλογής μεταξύ πολλών δυνατοτήτων.³² Τα ατομικά δικαιώματα δεν έχουν τη λειτουργία να προστατεύσουν καθαυτά την αξιοπρέπεια, αλλά να δημιουργήσουν και να διατηρήσουν τις προϋποθέσεις αυτής. Στην αξία του ανθρώπου ανήκει η ελευθερία της επικοινωνίας σε σχέση με τις πληροφορίες που ανταλλάσσει. Η εσωτερική ολοκλήρωση ενός ανθρώπου προϋποθέτει μεταξύ άλλων, την ελευθερία της επικοινωνίας, την ελευθερία στην παροχή και πρόσληψη πληροφοριών και η καταγραφή προσωπικών πληροφοριών (με σκοπό τον έλεγχο και τη χειραγώγηση) προσβάλλει αυτήν καθαυτή την αξία του ανθρώπου, καθώς προσβάλλεται άμεσα η ελευθερία του να μην παίζει κανένα ρόλο ο οποίος προσδιορίζεται από τους άλλους.

Ωστόσο κατά την τελευταία ολοκληρωθείσα αναθεώρηση του Συντάγματος (2001), κρίθηκε επιβεβλημένη η κατοχύρωση ενός νέου, ειδικού δικαιώματος προστασίας των προσωπικών δεδομένων. Το νέο άρθρο 9Α του ελληνικού Συντάγματος 1975/86/01 που περιλήφθηκε στο Σύνταγμα με την τελευταία αναθεώρηση του 2001 ορίζει ότι “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 νόμος ορίζει”.³³

Η συνταγματική κατοχύρωση έχει καταρχήν ένα συμβολικό βάρος και ρόλο, τόσο επειδή ανάγει την προστασία προσωπικών δεδομένων σε αυτοτελές δικαίωμα, όσο και επειδή τεκμηριώνει την προσαρμογή και την αντίδραση της έννομης τάξης στις ραγδαίες μεταβολές που προκαλεί στο κοινωνικό γίγνεσθαι η εξέλιξη της τεχνολογίας. Το δικαίωμα προστασίας προσωπικών δεδομένων εντάσσεται στα νέα δικαιώματα που

³² Βαθρακοκόιλη Β., << Ερμηνεία Αστικού Κώδικα, Τόμος Α>>, 2001 ,σελ.269

³³ Σωτηρόπουλος Β., <<Η συνταγματική προστασία των προσωπικών δεδομένων >>, 2006, σελ.9

προέκυψαν από τη συνταγματική αναθεώρηση, κοινό χαρακτηριστικό των οποίων είναι η μέριμνα για τη διαφύλαξη της προσωπικής αυτονομίας και τη θωράκιση του ήδη γνωστού χώρου αυτοκαθορισμού³⁴ σε συνθήκες οικονομικής ανάπτυξης και αξιοποίησης της τεχνολογίας. Η ειδική συνταγματική διάταξη διαδηλώνει και ταυτόχρονα κατοχυρώνει με τον καλύτερο και πληρέστερο τρόπο την ιδιαίτερη αξία του δικαιώματος, δηλ. τη σημασία που έχει η περιοριστική και περιορισμένη από τα δικαιώματα του προσώπου χρήση των προσωπικών δεδομένων, για τις προϋποθέσεις ανάπτυξης και αυτόνομης δράσης ενός προσώπου μέσα σε μία κοινωνία, κύριο χαρακτηριστικό της οποίας είναι η ραγδαία τεχνολογική ανάπτυξη.

Η προστασία προσωπικών δεδομένων ανήκει στην κατηγορία των νέων δικαιωμάτων που κατοχυρώνει το αναθεωρημένο Σύνταγμα, κοινό στοιχείο των οποίων είναι η εξασφάλιση όχι μόνο έναντι της κρατικής εξουσίας αλλά και έναντι των ιδιωτών. Η πλέον, ή μάλλον η μόνη, συγκεκριμένη απόφαση του αναθεωρητικού νομοθέτη σχετικά με τις εγγυήσεις προστασίας των προσωπικών δεδομένων αφορά τη συνταγματική κατοχύρωση της ανεξάρτητης Αρχής με αποστολή τη διασφάλιση του δικαιώματος. Η επιλογή αυτή του αναθεωρητικού νομοθέτη έχει ως αφετηρία α) τη διαπίστωση ότι υπό τις δεδομένες συνθήκες εξέλιξης των νέων τεχνολογιών και επέκτασης της επεξεργασίας προσωπικών δεδομένων, ούτε οι κλασικοί ελεγκτικοί μηχανισμοί, ούτε τα μεμονωμένα άτομα είναι σε θέση να εξασφαλίσουν αποτελεσματικά την προστασία των προσωπικών δεδομένων, ανεξάρτητα εάν οι σχετικές επιταγές απορρέουν από τον θεμελιώδη ή τον κοινό νόμο και β) τη συνειδητή επιλογή της θεσμικής θωράκισης του νέου αυτού δικαιώματος.

Αξίζει να σημειωθεί ότι η ίδρυση ανεξάρτητων αρχών αποτυπώνεται ως εγγενές χαρακτηριστικό του συστήματος προστασίας των προσωπικών δεδομένων σε πρόσφατα διεθνή κείμενα, δεσμευτικά και μη. Ως προς την ανεξάρτητη αρχή το Σύνταγμα δεν επιτάσσει παρά τον ανεξάρτητο χαρακτήρα της, στοιχείο που προσδιορίζεται εγγύτερα στο άρθρο 101 Α, δια της αναφοράς στην προσωπική και λειτουργική ανεξαρτησία.³⁵ Η ανεξαρτησία είναι συστατικό στοιχείο της έννοιας του ελέγχου και νοείται ως το

³⁴ Καράκωστα Ι, Το δίκαιο του Ίντερνετ (Νομική αντιμετώπιση του διαδικτύου), ΝοΒ 1998, σελ.1172

³⁵ www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-105/ (08/04/2013)

σύνολο των θεσμικών και λειτουργικών προϋποθέσεων που καθιστούν δυνατή την επιδίωξη των ειδικών σκοπών του ελέγχου και πιθανή την επίτευξή τους. Εκτός από την θετική επιταγή προς τον νομοθέτη για ίδρυση και διατήρηση μιας τέτοιας αρχής, η διάταξη αυτή δηλώνει ότι τυχόν περιορισμός των αρμοδιοτήτων, εξουσιών και ευχερειών της ελεγκτικής αρχής σε βαθμό που δεν μπορεί πλέον να διασφαλιστεί η αποτελεσματική προστασία του δικαιώματος, προφανώς δεν θα ανταποκρίνεται στις προσδοκίες του αναθεωρητικού νομοθέτη.

2.2 Ο νόμος 2472/1997

Ο Νόμος 2472/1997³⁶ έχει ως αντικείμενο τη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων. Παράλληλα συνδέεται με τις συνταγματικά κατοχυρωμένες αρχές του σεβασμού της προσωπικότητας (άρθρ.2 παρ.1 και 5 παρ.1 Σ) του απαραβίαστου της ιδιωτικής ζωής του ατόμου (αρθρ.9Σ), καθώς και του απορρήτου των επικοινωνιών (αρθρ.19 Σ).Ο νόμος αυτός περιέχει κανόνες ουσιαστικούς, διαδικαστικούς και κυρωτικούς που θεσμοθετούν ένα κανονιστικό πλαίσιο το οποίο οριοθετεί συνταγματικά ανεκτή επεξεργασία δεδομένων προσωπικού χαρακτήρα, με στόχο την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και της ιδιωτικής ζωής.

³⁶ Κατά τον Ι.Δ. Ιγγλεζάκη πρόκειται για νόμο εκτελεστικό του Συντάγματος, καθώς το περιεχόμενο του αποτελεί εξειδικευμένη μορφή της συνταγματικής αρχής του άρθρου 9 Α περί προστασίας του ατόμου από τη συλλογή, αποθήκευση και επεξεργασία των προσωπικών δεδομένων και καθίσταται σαφές και από τη διατύπωση του ίδιου του άρθρου 9 Α, στο οποίο προβλέπεται επιφύλαξη υπέρ του νόμου.

2.2.1 Βασικές έννοιες του Ν.2472/1997

Ως δεδομένα προσωπικού χαρακτήρα³⁷ νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, σε ατομικά ορισμένο δηλαδή φυσικό πρόσωπο και του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα. Δε λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα των δεδομένων. Δηλαδή τα δεδομένα αυτά αν δεν εξατομικεύουν το φυσικό πρόσωπο στο οποίο αναφέρονται, δεν απασχολούν τον νόμο.

Ακόμη μια κατηγορία δεδομένων είναι τα λεγόμενα ευαίσθητα δεδομένα, τα οποία αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις τη συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και την ερωτική ζωή, καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.³⁸

Υποκείμενο των δεδομένων είναι το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί άμεσα ή έμμεσα.

Ο όρος επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με το (άρθρο 2 στοιχεία δ) του νόμου, νοείται κάθε εργασία, ή σειρά εργασιών, που πραγματοποιείται από δημόσιο ή νομικό πρόσωπο, δημοσίου ή ιδιωτικού δικαίου, ή ένωση προσώπων, ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και

³⁷ Σε αυτό το σημείο πρέπει να γίνει διάκριση του όρου « προσωπικά δεδομένα» και «δεδομένα προσωπικού χαρακτήρα», όροι που συγχέονται ευρύτατα στη πράξη αλλά όμως δε ταυτίζονται εννοιολογικά, καθώς η βασική τους διαφορά συνοψίζεται στο εξής: τα «προσωπικά δεδομένα» μπορεί να είναι και δεδομένα μη προσωπικού χαρακτήρα που απλά ο κάτοχος τους τα θεωρεί προσωπικά του, π.χ. το δοκίμιο ενός συγγραφέα ,που δεν περιέχει πληροφορίες που αφορούν στο πρόσωπο του ίδιου του συγγραφέα, αλλά στο θέμα το οποίο ο συγγραφέας πραγματεύεται. Αντιθέτως ο Όρος «δεδομένα προσωπικού χαρακτήρα», περιλαμβάνει τα δεδομένα εκείνα τα οποία πράγματι έχουν «προσωπικό χαρακτήρα» και αυτά είναι μόνο που προστατεύονται από το νόμο, καθώς ο νόμος δεν ενδιαφέρεται για το τι υποκειμενικά θεωρεί κάθε άτομο ως προσωπικά του δεδομένα.

³⁸ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων,2001, σελ.6.

εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα , όπως η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση, η αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση, ή κάθε λογής άλλης μορφής διάθεση, συσχέτιση και συνδυασμός.³⁹

Οι παραπάνω εργασίες που συνιστούν την «επεξεργασία» κατά την έννοια του νόμου διακρίνονται σε τρία στάδια.⁴⁰ Το πρώτο στάδιο αφορά στη συλλογή των δεδομένων προσωπικού χαρακτήρα, το δεύτερο στάδιο περιλαμβάνει τις εργασίες που αφορούν την επεξεργασία, όπως για παράδειγμα η οργάνωση, η διατήρηση, η αποθήκευση, η τροποποίηση, η διαγραφή και η καταστροφή των δεδομένων, ενώ το τρίτο στάδιο αφορά στη χρήση των αποτελεσμάτων του προηγούμενου σταδίου, όπως την εξαγωγή, τη διαβίβαση ή την κάθε άλλης μορφής διάθεση.

Τα πρόσωπα στα οποία αναφέρονται οι ρυθμίσεις αυτές του νόμου είναι τα εξής:

- Υπεύθυνος επεξεργασίας: οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία και οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις του νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο⁴¹.
- Ο εκτελών την επεξεργασία: οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπευθύνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός. Υπάρχει μια διάκριση μεταξύ εκτελούντος και υπευθύνου επεξεργασίας, συνίσταται στις περιπτώσεις που οι οργανισμοί αποφασίζουν να αναθέσουν σε τρίτους τη διενέργεια συγκεκριμένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που ήδη κατέχουν, επειδή δε διαθέτουν οι ίδιοι την

³⁹ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.8.

⁴⁰ Ε. Παπακωνσταντίνου, Νομικά Θέματα Πληροφορικής, 2006, σελ 32-33.

⁴¹ www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#2 (08/04/2013)

απαραίτητη τεχνογνωσία ή για λόγους μείωσης του κόστους. Όλοι αυτή η διαδικασία ονομάζεται outsourcing. Η σχέση που μπορεί να συνδέει τον υπεύθυνο επεξεργασίας και τον εκτελούντα είναι η σύμβαση έργου, πάντως ο εκτελών την επεξεργασία θα πρέπει να βρίσκεται υπό την άμεση εποπτεία του υπευθύνου.

- Τρίτος: θεωρείται κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, η οποιοσδήποτε άλλος οργανισμός ο οποίος εμπλέκεται σε επεξεργασία δεδομένων προσωπικού χαρακτήρα από την πλευρά των διενεργούντων την επεξεργασία, χωρίς να είναι ο ίδιος υπεύθυνος επεξεργασίας, ούτε ο εκτελών την επεξεργασία. Δηλαδή ο τρίτος πρέπει απαραίτητα να τελεί υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας, δεν είναι όμως όπως είπαμε το πρόσωπο που εκτελεί την επεξεργασία.
- Αποδέκτης: είναι το φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο η όχι. Με λίγα λόγια αποδέκτης είναι αυτός που λαμβάνει τα αποτελέσματα της επεξεργασίας.

Άλλοι όροι που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι οι εξής:

- Αρχείο δεδομένων προσωπικού χαρακτήρα: σύμφωνα με το άρθρο 2 του νόμου είναι το σύνολο δεδομένων προσωπικού χαρακτήρα, τα οποία αποτελούν ή μπορεί να αποτελέσουν αντικείμενο επεξεργασίας, και τα οποία τηρούνται από το δημόσιο ή από νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου, ή ένωση προσώπων, ή φυσικό πρόσωπο.⁴²
- Διασύνδεση: νοείται η μορφή επεξεργασίας που συνίσταται στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου ή αρχείων που τηρούνται από άλλους υπεύθυνους επεξεργασίας, ή που τηρούνται από τον ίδιο υπεύθυνο επεξεργασίας για άλλο σκοπό.

⁴² www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#2 (08/04/2013)

- Συγκατάθεση του υποκειμένου των δεδομένων: είναι η κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και εν πλήρη επίγνωση, με την οποία το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Η ενημέρωση αυτή περιλαμβάνει πληροφόρηση τουλάχιστον για το σκοπό της επεξεργασίας, τα δεδομένα ή τις κατηγορίες δεδομένων που αφορά η επεξεργασία, τους αποδέκτες ή τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα, καθώς και το όνομα, την επωνυμία και τη διεύθυνση του υπευθύνου επεξεργασίας και του τυχόν εκπροσώπου του. Η συγκατάθεση μπορεί να ανακληθεί οποτεδήποτε, χωρίς αναδρομικό αποτέλεσμα.⁴³

2.2.2 Επεξεργασία δεδομένων.

Για να γίνεται νόμιμα η επεξεργασία θα πρέπει τα δεδομένα να συλλέγονται με νόμιμο και θεμιτό τρόπο, και να χρησιμοποιούνται για νομίμους, σαφείς και καθορισμένους σκοπούς. Τα δεδομένα θα πρέπει να είναι ενήμερα, ακριβή και συναφή με το σκοπό για τον οποίον έχουν συλλεχθεί. Η διατήρηση των δεδομένων σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας του υποκειμένου θα πρέπει να γίνεται μόνο κατά την περίοδο που απαιτείται για την πραγματοποίηση του σκοπού για τον οποίο έχουν συλλεχθεί, μετά την πάροδο αυτής της περιόδου η διατήρηση επιτρέπεται μόνο από την Αρχή, για επιστημονικούς ή στατιστικούς σκοπούς, εφόσον δεν θίγονται τα δικαιώματα του υποκειμένου.

Η συλλογή θα πρέπει να γίνεται με τη συγκατάθεση⁴⁴ του υποκειμένου των δεδομένων, και κατ' εξαίρεση⁴⁵ επιτρέπεται για δημόσιο συμφέρον, για την εκπλήρωση σύμβασης της οποίας το υποκείμενο είναι συμβαλλόμενο μέρος, για τη διαφύλαξη

⁴³ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.9

⁴⁴ Ιγγλεζάκης Ι., Ευαίσθητα προσωπικά δεδομένα, 2003, σελ.70

⁴⁵ Ιγγλεζάκης Ι., Ευαίσθητα προσωπικά δεδομένα, 2003λ.72

ζωτικού συμφέροντος του υποκειμένου, για την εκπλήρωση υποχρεώσεων του υπευθύνου επεξεργασίας που επιβάλλονται από το νόμο, και όταν η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος του υπεύθυνου επεξεργασίας ή τρίτων στους οποίους ανακοινώνονται τα δεδομένα.⁴⁶

Ο υπεύθυνος επεξεργασίας θα πρέπει να γνωστοποιήσει στην Αρχή τη σύσταση και λειτουργία αρχείου δεδομένων και να δηλώσει το ονοματεπώνυμο του, τη διεύθυνση που είναι εγκατεστημένο το αρχείο, το σκοπό, το είδος των δεδομένων, το χρονικό διάστημα που θα εκτελείται η επεξεργασία, καθώς επίσης και τους αποδέκτες των δεδομένων. Τα στοιχεία αυτά καταχωρούνται στο Μητρώο Αρχείων και Επεξεργασιών που τηρεί η Αρχή, η οποία θα πρέπει να ενημερώνεται για κάθε μεταβολή των στοιχείων αυτών. Ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση γνωστοποίησης όταν η επεξεργασία πραγματοποιείται αποκλειστικά για σκοπούς που συνδέονται άμεσα με σχέση εργασίας ή παροχή υπηρεσιών προς το δημόσιο, όταν η επεξεργασία αφορά πελάτες ή προμηθευτές εφόσον τα δεδομένα δεν κοινοποιούνται σε τρίτους, όταν η επεξεργασία αφορά μέλη σωματίων, ενώσεων, πολιτικών κομμάτων και έχουν δώσει τη συγκατάθεση τους και όταν η επεξεργασία γίνεται από γιατρούς και αφορά ιατρικά δεδομένα και δικηγόρους ή συμβολαιογράφους και αφορά παροχή υπηρεσιών σε πελάτες τους.⁴⁷

Η διαβίβαση των δεδομένων σε χώρες της Ευρωπαϊκής Ένωσης είναι ελεύθερη. Σε χώρες εκτός Ευρωπαϊκής Ένωσης επιτρέπεται μόνο μετά από άδεια της Αρχής, εάν κριθεί ότι η χώρα στην οποία διαβιβάζονται τα δεδομένα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας.⁴⁸

Ο νόμος προβαίνει σε μία περαιτέρω εξειδίκευση διαχωρίζοντας τα ευαίσθητα προσωπικά δεδομένα. Και θεσπίζει γενική απαγόρευση της επεξεργασίας τους. Ως «Ευαίσθητα δεδομένα», θεωρούνται τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις,

⁴⁶ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.13.

⁴⁷ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.19.

⁴⁸ www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#9 (08/04/2013)

στη συμμετοχή σ συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Κατ' εξαίρεση όμως, επιτρέπεται η συλλογή και η επεξεργασία τους, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής.⁴⁹

Το υποκείμενο των δεδομένων έχει το δικαίωμα της ενημέρωσης, το δικαίωμα της πρόσβασης, το δικαίωμα της αντίρρησης ή διόρθωσης και το δικαίωμα της δικαστικής προστασίας. Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει⁵⁰ το υποκείμενο των δεδομένων με τρόπο πρόσφορο και σαφή για την ταυτότητα του και τυχόν εκπροσώπων του, για το σκοπό της επεξεργασίας, τους αποδέκτες των δεδομένων και την ύπαρξη του δικαιώματος πρόσβασης. Εάν για την συλλογή των δεδομένων ο υπεύθυνος επεξεργασίας ζητεί τη συνδρομή του υποκειμένου θα πρέπει να τον ενημερώσει ειδικώς και εγγράφως για τα στοιχεία των άρθρων 11 έως και 13 του παρόντος νόμου. Με απόφαση της Αρχής μπορεί να αρθεί η υποχρέωση ενημέρωσης για λόγους εθνικής ασφάλειας, ή για την διακρίβωση ιδιαίτερα σοβαρών αδικημάτων. Η υποχρέωση ενημέρωσης δεν υφίσταται όταν η συλλογή γίνεται για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα.⁵¹

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας με τρόπο σαφή και κατανοητό όλα τα δεδομένα που τον αφορούν καθώς και την προέλευση τους, τον σκοπό και την εξέλιξη της επεξεργασίας καθώς και τους αποδέκτες των δεδομένων. Το δικαίωμα της πρόσβασης ασκείται με την υποβολή σχετικής αίτησης στον υπεύθυνο επεξεργασίας και την καταβολή χρηματικού ποσού το ύψος του οποίου καθορίζεται από την Αρχή. Ο υπεύθυνος έχει την υποχρέωση εντός 15 ημερών να απαντήσει στον αιτούντα σε γλώσσα κατανοητή. Σε περίπτωση άρνησης ή μη ικανοποιητικής απάντησης, το υποκείμενο των δεδομένων έχει το δικαίωμα να προσφύγει στη Αρχή. Με απόφαση της Αρχής μπορεί να αρθεί το

⁴⁹ Τουντόπουλος Β, Η διασύνδεση αρχείων στον.2472/1997, ΝοΒ 1999, σελ. 1242.

⁵⁰ Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων, ΔΕΕ, 1999, σελ.576.

⁵¹ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.24.

δικαίωμα της πρόσβασης για λόγους εθνικής ασφάλειας ή για την διακρίβωση ιδιαίτερα σοβαρών αδικημάτων.⁵²

Το δικαίωμα αντίρρησης⁵³ και διόρθωσης που έχει το υποκείμενο των δεδομένων ασκείται εγγράφως στον υπεύθυνο επεξεργασίας και πρέπει να περιέχει αίτημα για συγκεκριμένη ενέργεια, όπως διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση, μη διαβίβαση ή διαγραφή⁵⁴. Ο υπεύθυνος έχει την υποχρέωση εντός 15 ημερών να απαντήσει στον αιτούντα σε γλώσσα κατανοητή. Σε περίπτωση άρνησης ή μη ικανοποιητικής απάντησης το υποκείμενο των δεδομένων έχει το δικαίωμα να προσφύγει στη Αρχή. Εάν η Αρχή πιθανολογήσει ότι οι αντιρρήσεις είναι εύλογες και ότι συντρέχει σοβαρός λόγος βλάβης του υποκειμένου από τη συνέχιση της επεξεργασίας μπορεί να επιβάλει την άμεση αναστολή της επεξεργασίας έως να εκδώσει οριστική απόφαση. Η Αρχή τηρεί μητρώο στο οποίο καθένας μπορεί να δηλώσει ότι τα στοιχεία του δεν επιθυμεί να αποτελέσουν αντικείμενο επεξεργασίας για λόγους προώθησης πωλήσεων ή εξ' αποστάσεως παροχής υπηρεσιών. Οι υπεύθυνοι επεξεργασίας των σχετικών αρχείων θα πρέπει να συμβουλευονται το μητρώο της Αρχής πριν από κάθε επεξεργασία και να διαγράφουν από τις λίστες τους τα πρόσωπα της παραγράφου αυτής.⁵⁵

Καθένας έχει το δικαίωμα να ζητήσει από το αρμόδιο κάθε φορά δικαστήριο την άμεση αναστολή ή μη εφαρμογή απόφασης που τον θίγει, την οποία έχει λάβει διοικητική αρχή, νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου ή φυσικό πρόσωπο αποκλειστικά με αυτοματοποιημένη επεξεργασία στοιχείων, εφόσον η επεξεργασία αυτή αποβλέπει σε αξιολόγηση της προσωπικότητας του και ιδίως της αποδοτικότητας του στην εργασία και της αξιοπιστίας του. Το δικαίωμα μπορεί να χρησιμοποιηθεί και

⁵² Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.26.

⁵³ Αλεξανδροπούλου –Αιγυπτιάδου Ε., Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου τους, Αρμ., 2005, σελ.137.

⁵⁴ www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#13 (08/04/2013)

⁵⁵ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.26.

όταν δεν συντρέχουν οι λοιπές ουσιαστικές προϋποθέσεις της προσωρινής δικαστικής προστασίας, όπως προβλέπονται κάθε φορά.⁵⁶

Σύμφωνα με το άρθρο 15 του Νόμου συνιστάται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Αρχή), με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά. Η Αρχή αποτελεί ανεξάρτητη δημόσια αρχή, και εξυπηρετείται από δική της γραμματεία και δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο.

Η Αρχή έχει ως αρμοδιότητες:

- Έκδοση οδηγιών που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας ή τους τυχόν εκπροσώπους τους και δίδει κατά την κρίση της δημοσιότητα σε αυτές.
- Χορηγεί τις άδειες που προβλέπουν οι διατάξεις του παρόντος νόμου και καθορίζει το ύψος των σχετικών παράβολων.
- Καταγγέλλει τις παραβάσεις των διατάξεων του παρόντος νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.
- Επιβάλλει τις κατά το άρθρο 21 του παρόντος νόμου διοικητικές κυρώσεις.
- Ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους, στο πλαίσιο των οποίων ελέγχονται η τεχνολογική υποδομή και άλλα, αυτοματοποιημένα ή μη μέσα που υποστηρίζουν την επεξεργασία των δεδομένων.
- Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

⁵⁶ www.dpa.gr/portal/page?_pageid=33.19052&_dad=portal&_schema=PORTAL#14 (08/04/2013)

- Εκδίδει κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο παρών νόμος.
- Συντάσσει κάθε χρόνο έκθεση για την εκτέλεση της αποστολής της κατά το προηγούμενο ημερολογιακό έτος. Στην έκθεση επισημαίνονται και οι τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Εξετάζει τα παράπονα των υποκειμένων των δεδομένων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων τους, όταν αυτά θίγονται από την επεξεργασία δεδομένων που τους αφορούν⁵⁷.

2.3 Ο νόμος 3471/2006

Ο νόμος 3471/2006⁵⁸ αφορά την προστασία δεδομένων προσωπικού χαρακτήρα και ιδιωτικής ζωής στον τομέα ηλεκτρονικών επικοινωνιών (ενσωμάτωση της οδηγίας 2002/58/EK του ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 12^{ης} Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, ΕΕ L 201/37 της 31^{ης} Ιουλίου 2002) καθώς και την τροποποίηση του ν.2472/1997.

Σκοπός των διατάξεων και των άρθρων του νόμου είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής, και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών.

⁵⁷ www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#15 (08/04/2013)

⁵⁸ www.et.gr/index.php?option=com_wrapper&view=wrapper&Itemid=108&lang=el (08/04/2013)

2.3.1 Βασικές έννοιες του νόμου 3471/2006

Στο άρθρο 2 του νόμου δίνονται οι ορισμοί κάποιων βασικών εννοιών οι οποίοι είναι:

- Συνδρομητής: νοείται κάθε φυσικό ή νομικό πρόσωπο που έχει συνάψει σύμβαση με φορέα παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.
- Χρήστης: νοείται κάθε φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών για την παροχή των υπηρεσιών αυτών.
- Δεδομένα κίνησης: νοούνται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών, ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης, η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας, καθώς και το δίκτυο από το οποίο προέρχεται ή καταλήγει η επικοινωνία.
- Δεδομένα θέσης: νοούνται τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.
- Επικοινωνία: νοείται κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών, μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Δεν περιλαμβάνονται πληροφορίες που διαβιβάζονται ως τμήμα ραδιοηλεκτρονικών υπηρεσιών στο κοινό μέσω δικτύου ηλεκτρονικών επικοινωνιών, εκτός από τις περιπτώσεις κατά τις οποίες οι

πληροφορίες μπορούν να αφορούν αναγνωρίσιμο συνδρομητή ή χρήστη που τις λαμβάνει.

- Κλήση: νοείται η σύνδεση που πραγματοποιείται μέσω μιας διαθέσιμης στο κοινό τηλεφωνικής υπηρεσίας, που επιτρέπει αμφίδρομη επικοινωνία σε πραγματικό χρόνο.
- Υπηρεσία προστιθεμένης αξίας: νοείται κάθε υπηρεσία η οποία επιβάλλει την επεξεργασία δεδομένων κίνησης ή δεδομένων θέσης, πέραν εκείνων που απαιτούνται για την μετάδοση μιας επικοινωνίας με τη χρέωση της.
- Ηλεκτρονικό ταχυδρομείο: νοείται κάθε μήνυμα με κείμενο, φωνή, ήχο ή εικόνα που αποστέλλεται μέσω δημοσίου δικτύου επικοινωνιών, το οποίο μπορεί να αποθηκεύεται στο δίκτυο ή στον τερματικό εξοπλισμό του παραλήπτη, έως ότου ληφθεί από τον παραλήπτη.
- Υπηρεσίες ηλεκτρονικών επικοινωνιών: νοούνται οι υπηρεσίες που προέρχονται συνήθως έναντι αμοιβής και των οποίων η παροχή συνίσταται, εν λόγο η εν μέρει, στη μεταφορά σημάτων σε δίκτυα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων των υπηρεσιών τηλεπικοινωνιών και των υπηρεσιών μετάδοσης σε δίκτυα που χρησιμοποιούνται για ραδιοτηλεοπτικές μεταδόσεις. Στις υπηρεσίες ηλεκτρονικών επικοινωνιών δεν περιλαμβάνονται υπηρεσίες παροχής ή ελέγχου περιεχομένου που μεταδίδεται μέσω δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών⁵⁹.
- Δημόσιο δίκτυο επικοινωνιών: νοείται το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.
- Διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών: νοούνται οι υπηρεσίες ηλεκτρονικών επικοινωνιών που παρέχονται στο κοινό.

⁵⁹ www.dsnet.gr/Epikairothta/Nomothesia/n3471_06.htm (08/04/2013)

2.3.2 Επεξεργασία δεδομένων

Ο νόμος προβλέπει ότι οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης προστατεύεται από το απόρρητο των επικοινωνιών, και απαγορεύει την υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών. Η καταγραφή συνδιαλέξεων επιτρέπεται όταν γίνεται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων εμπορικής συναλλαγής ή άλλης επικοινωνίας επαγγελματικού χαρακτήρα, υπό την προϋπόθεση ότι και τα δύο μέρη, μετά από προηγούμενη ενημέρωση σχετικά με το σκοπό της καταγραφής, παρέχουν τη συγκατάθεση τους⁶⁰ και θα πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της.

Απαγορεύεται η χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, με την εγκατάσταση κατασκοπευτικών λογισμικών, κρυφών αναγνωριστικών στοιχείων και άλλων παρόμοιων διατάξεων.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν ο χρήστης έχει δώσει την συγκατάθεση του, μετά από ενημέρωση για το είδος των δεδομένων, το σκοπό και την έκταση της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες αποδεκτών, ή όταν η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία ο συνδρομητής ή ο χρήστης είναι συμβαλλόμενο μέρος, ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, μετά από αίτηση του συνδρομητή. Η ενημέρωση αποτελεί μία από τις πιο σημαντικές προϋποθέσεις της νομιμότητας της

⁶⁰ www.dsnet.gr/Epikairothta/Nomothesia/n3471_06.htm (08/04/2013)

επεξεργασίας, καθώς παρά το ότι χρησιμοποιείται σαν γενικός όρος, αποτελείται από την συναίνεση και από την έγκριση.⁶¹

Ο φορέας παροχής δημοσίου δικτύου ή και διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών δεν επιτρέπεται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα και τα δεδομένα κίνησης και θέσης ή να τα διαβιβάζει σε τρίτους για άλλους σκοπούς, εκτός εάν ο συνδρομητής ή ο χρήστης έχει ρητά και ειδικά δώσει τη συγκατάθεση του. Εξειδίκευση της ελευθερίας της συγκατάθεσης αποτελεί το άρθρο 10 αρ. 4 β εδ. 4 ν. 3271/2006, όπου αναφέρεται πως «Δεν επιτρέπεται στους φορείς παροχής υπηρεσιών δημοσίων καταλόγων να εξαρτούν την παροχή των υπηρεσιών δημοσίου καταλόγου από τη συγκατάθεση του συνδρομητή για τη διαβίβαση των δεδομένων για σκοπούς άλλους από αυτούς για τους οποίους έχουν συλλεγεί».⁶²

Όταν τα δεδομένα διαβιβάζονται σε τρίτους, η συγκατάθεση απαιτείται να είναι έγγραφη και μπορεί να ανακληθεί οποτεδήποτε. Αν ανακληθεί και εφόσον τα δεδομένα έχουν εν τω μεταξύ ανακοινωθεί σε τρίτους, η ανάκληση ανακοινώνεται σε αυτούς με φροντίδα του υπεύθυνου επεξεργασίας. Ο νομοθέτης, όσον αφορά τον τρόπο και χρόνο ανάκλησης της δήλωσης συγκατάθεσης, με την λέξη «οποτεδήποτε» θέτει τον όρο της εύκολης τεχνικά και ατελούς για τον συνδρομητή/χρήστη δυνατότητας.⁶³

Η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.

Ο νόμος προβλέπει ποινικές κυρώσεις για όποιους χρησιμοποιούν, συλλέγουν, αποθηκεύουν, καταστρέφουν, μεταδίδουν και δημοσιοποιούν δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών. Οι παραβάτες τιμωρούνται με φυλάκιση

⁶¹ Αλεξανδροπούλου - Αιγυπτιάδου Ε., Προσωπικά δεδομένα, 2007, σελ.57.

⁶² Αλεξανδροπούλου - Αιγυπτιάδου Ε., Νομική διασφάλιση του απορρήτου των κινητών επικοινωνιών, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 2008, σελ.455.

⁶³ Χριστοδούλου Κ., Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, 2007, σελ.108.

τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον από δέκα χιλιάδων ευρώ (10.000) μέχρι και εκατό χιλιάδων ευρώ (100.000), αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.⁶⁴

2.4 Πεδίο εφαρμογής του Ν.2472/1997 και Ν.3471/2006

Οι ρυθμίσεις του ν.2472/1997, σύμφωνα με το άρθρο 3 παρ.1 του νόμου, βρίσκουν εφαρμογή σε κάθε είδους επεξεργασία δεδομένων, τόσο σε αυτοματοποιημένη όσο και σε μη, δηλαδή επεξεργασία με συμβατικές μεθόδους, στον ιδιωτικό και στο δημόσιο τομέα.

Επομένως, πρέπει να τονιστεί ότι η γενική νομοθεσία για την προστασία των προσωπικών δεδομένων, δηλαδή ο ν.2472/1997, ισχύει και εφαρμόζεται και στη συλλογή και επεξεργασία προσωπικών δεδομένων στο περιβάλλον του διαδικτύου, καθώς οι σχετικές διατάξεις εφαρμόζονται για κάθε επεξεργασία εν γένει, με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων.⁶⁵

Η αυτοματοποιημένη μέθοδος για επεξεργασία δεδομένων ή πληροφοριών στηρίζεται στις έννοιες του αλγορίθμου και του υπολογισμού, επομένως αυτοματοποιημένη νοείται η επεξεργασία που πραγματοποιείται σε υπολογιστικό περιβάλλον. Ο νομοθέτης ωστόσο, επέλεξε να διευρύνει το πεδίο εφαρμογής του νόμου και ως αυτοματοποιημένη θεωρείται και οποιαδήποτε άλλη επεξεργασία τελείται με ηλεκτρονικά μέσα όπως πχ τηλεοπτική εκπομπή, η αναπαραγωγή ηχογραφημάτων ή ψηφιακών φωτογραφιών.⁶⁶

⁶⁴ www.dsnet.gr/Epikairothta/Nomothesia/n3471_06.htm (08/04/2013)

⁶⁵ Α.Γ.Καϊσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.10.

⁶⁶ Ε. Παπακωνσταντίνου, Νομικά Θέματα Πληροφορικής, 2006, σελ 44.

Μη αυτοματοποιημένη επεξεργασία δεδομένων πραγματοποιείται με οποιονδήποτε άλλο τρόπο που δεν την καθιστά αυτοματοποιημένη. Οι διατάξεις αυτού του νόμου εφαρμόζονται στη μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο. Αντίθετα στην αυτοματοποιημένη επεξεργασία δεδομένων, ο νόμος εφαρμόζεται τόσο σε ένα μοναδικό προσωπικό δεδομένο (π.χ. ένα έγγραφο word η μια φωτογραφία), όσο και σε εκατομμύρια αυτών, οργανωμένα σε βάσεις δεδομένων. Γίνεται δεκτό ότι η επεξεργασία δεδομένων στο διαδίκτυο αποτελεί κατά κανόνα αυτοματοποιημένη επεξεργασία δεδομένων και άρα παρέλκει η εξέταση αν υπάρχει αρχείο.

Οι διατάξεις του παρόντος νόμου δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών η οικιακών.⁶⁷ Προσωπικές η οικιακές δραστηριότητες είναι εκείνες στις οποίες απουσιάζει το στοιχείο της εξωτερίκευσης και η χρήση τους γίνεται από το άτομο για σκοπούς μη εμπορικούς, όπως π.χ. η τήρηση οικιακών λογαριασμών, άλμπουμ φωτογραφιών, τήρηση τηλεφωνικού καταλόγου, όχι όμως και η ανάρτηση των παραπάνω στοιχείων στην προσωπική ιστοσελίδα του κατόχου της.⁶⁸ Στην περίπτωση αυτή δεν εφαρμόζεται καθόλου ο νόμος.

Σύμφωνα με το άρθρο 3 παρ.3 ν.2472/1997, ο νόμος εφαρμόζεται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν αυτή εκτελείται είτε: α) από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, εγκατεστημένο στην Ελληνική Επικράτεια ή σε τόπο, όπου εφαρμόζεται σύμφωνα με το δημόσιο διεθνές δίκαιο το ελληνικό δίκαιο, β) είτε από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην επικράτεια ή σε τόπο, όπου εφαρμόζεται το ελληνικό δίκαιο, όταν η επεξεργασία αφορά υποκείμενα εγκατεστημένα στην ελληνική επικράτεια. Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωση του προς την Αρχή εκπρόσωπο εγκατεστημένο στην ελληνική επικράτεια, ο οποίος υποκαθίσταται στα

⁶⁸ Ε. Παπακωνσταντίνου, Νομικά Θέματα Πληροφορικής, 2006, σελ 47.

δικαιώματα και υποχρεώσεις του υπευθύνου, χωρίς ο τελευταίος να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του.⁶⁹ Το ίδιο ισχύει και όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινική δίωξη. Τέλος ο νόμος αυτός εφαρμόζεται είτε από υπεύθυνο επεξεργασίας που δεν είναι εγκατεστημένος στην επικράτεια κράτους – μέλους της Ευρωπαϊκής Ένωσης ή κράτους του Ευρωπαϊκού Οικονομικού χώρου, αλλά τρίτης χώρας, και για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσφεύγει σε μέσα, αυτοματοποιημένα η όχι, εκτός αν τα μέσα αυτά χρησιμοποιούνται μόνο με σκοπό τη διέλευση από την Ελλάδα.⁷⁰ Δηλαδή, στη τελευταία αυτή περίπτωση, αν ο υπεύθυνος επεξεργασίας εκτός ΕΕ, επεξεργάζεται δεδομένα προσωπικού χαρακτήρα με μέσα που βρίσκονται στην Ελλάδα, ανεξαρτήτως αν τα δεδομένα αυτά αφορούν σε κατοίκους της χώρας ή αν ο ίδιος ο εκτελών την επεξεργασία είναι εγκατεστημένος στην Ελλάδα, τότε και πάλι εφαρμόζεται το ελληνικό δίκαιο.

Στη τελευταία αυτή περίπτωση όπως και στην προηγούμενη ο υπεύθυνος επεξεργασίας οφείλει να υποδείξει με γραπτή δήλωση του προς την αρχή, εκπρόσωπο εγκατεστημένο στην ελληνική επικράτεια, οποίος υποκαθίσταται στα δικαιώματα και τις υποχρεώσεις του υπευθύνου, χωρίς ο τελευταίος να απαλλάσσεται από τυχόν ιδιαίτερη ευθύνη του. Το ίδιο ισχύει όταν ο υπεύθυνος επεξεργασίας καλύπτεται από ετεροδικία, ασυλία ή άλλο λόγο που κωλύει την ποινική δίωξη.

Η παραπάνω ρύθμιση αναφέρεται κυρίως στον τόπο εγκατάστασης του υπευθύνου επεξεργασίας, δηλαδή στον τόπο πραγματικής άσκησης δραστηριότητας μέσω μονίμου καταστήματος και επομένως δεν ενδιαφέρει η έδρα του νομικού προσώπου της επιχείρησης που επεξεργάζεται προσωπικά δεδομένα.

Ο Ν.3471/2006 όπως προαναφέραμε έχει σκοπό την προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και τη θέσπιση των

⁶⁹ Α.Γ. Καΐσης - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001, σελ.11.

⁷⁰ Η εξαίρεση της διέλευσης αποκτά νόημα στο σύγχρονο διαδικτυακό περιβάλλον- αν οι επικοινωνιακοί κόμβοι διέρχονται από τη χώρα, αυτό δεν σημαίνει ότι βέβαια ότι τα δεδομένα που περνούν από αυτούς θα διέπονται από το ελληνικό δίκαιο.

προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών. Ο Ν. 3471/2006, λοιπόν βρίσκει εφαρμογή κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών, στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών (άρθρο 3 παρ.1). Εδώ υπάγεται ένα σύνολο υπηρεσιών, μεταξύ των οποίων και οι υπηρεσίες που παρέχονται μέσω διαδικτύου, και όσες παρέχονται μέσω κινητών ψηφιακών δικτύων. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται στο πλαίσιο μη διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, εφαρμόζεται ο ν.2472/1997, όπως ισχύει.

Οι διατάξεις 8 και 9 του ν.3471/2006⁷¹ εφαρμόζονται στις γραμμές συνδρομητών που συνδέονται με ψηφιακά κέντρα και, όταν αυτό είναι τεχνικώς εφικτό, σε γραμμές συνδρομητών που συνδέονται με αναλογικά κέντρα, εφόσον τούτο δεν συνεπάγεται δυσανάλογη οικονομική επιβάρυνση. Η εθνική επιτροπή τηλεπικοινωνιών και ταχυδρομείων διαπιστώνει τις περιπτώσεις όπου η σύνδεση με αναλογικά κέντρα είναι τεχνικώς αδύνατη η απαιτεί δυσανάλογη επένδυση, και ενημερώνει σχετικός την ευρωπαϊκή επιτροπή.

Σε αντίθεση με το Ν.2472/1997, ο Ν. 3471/2006 εφαρμόζεται και όταν ακόμη οι συνδρομητές είναι νομικά πρόσωπα. Επίσης αξίζει να αναφερθεί ότι οι διατάξεις που αφορούν την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα δεν παρουσιάζουν αυτοτέλεια, αλλά εντάσσονται στο γενικότερο πλαίσιο των ρυθμίσεων του ν.2472/97.

Συνεπώς, κύριο κορμό της προστασίας προσωπικών δεδομένων και στο περιβάλλον του διαδικτύου αποτελεί η γενική νομοθεσία για την προστασία των προσωπικών δεδομένων, δηλαδή ο Ν.2472/97, ενώ Ν.3471/2006 ισχύει παράλληλα και εφαρμόζεται εισάγοντας και ειδικότερες ρυθμίσεις. Οι διατάξεις του Ν.2472/1997

⁷¹www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/%CE%9DOMOTHESIA%20PROSOPIKA%20DEDOMENA_GREEK/3471_06_MAY2012FINAL.PDF (09/04/2013)

εφαρμόζονται σε κάθε ζήτημα που δε ρυθμίζεται ειδικότερα από το Ν. 3471/2006, σύμφωνα με το άρθρο 3παρ2 του Ν.3471/2006.

ΚΕΦΑΛΑΙΟ: 3 ΤΟ ΔΙΕΘΝΕΣ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

3.1 Η.Π.Α. [ΛΙΛΕΣ]

Στις Η.Π.Α. το σύνταγμα δεν περιέχει ειδική διάταξη για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, υπάρχουν ποικίλα νομοθετήματα που ρυθμίζουν επιμέρους θέματα, αλλά η συνολική προστασία που παρέχεται στο άτομο εμφανίζει κενά. Το Αμερικανικό Ανώτατο Δικαστήριο έχει καταλήξει στην ερμηνεία ότι η Διακήρυξη των Δικαιωμάτων δημιουργεί τις προϋποθέσεις προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων. Η συνήθης πρακτική στις Η.Π.Α. είναι να αντιμετωπίζονται οι παραβιάσεις όταν εμφανίζονται, σε αντίθεση με την Ευρώπη, όπου η νομοθεσία επιδιώκει την πρόληψη της παραβίασης. Ακολουθείται μια φιλελεύθερη προσέγγιση που επιτρέπει την αυτορύθμιση σε κάθε κλάδο, δίνοντας έτσι τη δυνατότητα σε φορείς και επιχειρήσεις να δρουν κατά βούληση και να χρησιμοποιούν δικό τους πλαίσιο κανόνων. Η χρήση των προσωπικών πληροφοριών από τις κρατικές υπηρεσίες καθορίζεται από το νόμο για την προστασία του ιδιωτικού βίου privacy act του 1974 ο οποίος θεσπίζει μια σειρά αρχών για τη χρήση των προσωπικών πληροφοριών, καθώς και από νόμους που ρυθμίζουν επιμέρους θέματα.

3.1.1 Το σύνταγμα των Η.Π.Α.

Στης Η.Π.Α. το σύνταγμα δεν προβλέπει ρητά το θεμελιώδες δικαίωμα στην ιδιωτική ζωή, υποστηρίζεται ότι η πρώτη, η τρίτη, η τέταρτη, η πέμπτη και η δέκατη τέταρτη τροποποίηση του συντάγματος προστατεύουν το δικαίωμα αυτό. Στην πρώτη τροποποίηση αναφέρεται το δικαίωμα του να μπορεί κανείς να εκφράζεται ανώνυμα και να μην αποκαλύπτει τη συμμετοχή του σε ενώσεις. Η τρίτη αναφέρεται στην προστασία του ασύλου της κατοικίας. Η τέταρτη τροποποίηση καθορίζει το ενδιαφέρον της ιδιωτικής ζωής, αναγνωρίζοντας το δικαίωμα των πολιτών των Η.Π.Α. να είναι ασφαλείς τα σπίτια τους και τα έγγραφα τους από αυθαίρετες παρεμβάσεις του κράτους, και κανένα ένταλμα δεν εκδίδεται παρά μόνο όταν υπάρχουν σοβαρές ενδείξεις που βασίζονται σε όρκο ή έγγραφη μαρτυρία και περιγράφονται σε αυτό, ο χώρος διεξαγωγής της έρευνας, και τα πρόσωπα ή τα αντικείμενα που πρόκειται να κατασχεθούν.⁷² Το γεγονός αυτό προβληματίζει διότι η προστασία της ιδιωτικής ζωής βασίζεται στην χρήση του κριτηρίου της εμπιστοσύνης. Με βάση την 4η τροποποίηση, η απόφαση *Olmsted* κατά των Η.Π.Α (*Olmstead v. United States*, 277 U.S. 438), όπου το δικαστήριο αποφάσισε ότι η παγίδευση τηλεφώνου από την αστυνομία δεν αποτελούσε παραβίαση της 4ης τροποποίησης. Ομοίως και η απόφαση *Katz* κατά Η.Π.Α (*Katz v. United States*, 389 U.S. 347) η οποία ανέτρεψε την προηγούμενη απόφαση και διατύπωσε την άποψη ότι η παγίδευση δημοσίου τηλεφώνου είναι αντίθετη στην 4^η τροποποίηση, αφού υπήρχε για τον χρήστη «εύλογη προσδοκία ιδιωτικότητας», αποτέλεσαν τις σημαντικότερες αποφάσεις αναφοράς στο δικαίωμα στην ιδιωτικότητα, το οποίο δεν προστατεύεται ρητά από το Αμερικάνικο σύνταγμα⁷³.

Η Πέμπτη αφορά την προσωπική του ασφάλεια. Η ένατη κατοχυρώνει τη δυνατότητα διάπλασης άγραφων δικαιωμάτων στο λαό, και το κύριο κανονιστικό θεμέλιο του δικαιώματος στην ιδιωτική ζωή, και η δέκατη τέταρτη θεμελιώνει την

⁷² www.legal-dictionary.thefreedictionary.com/Fourth+Amendment (08/02/2012)

⁷³ www.fourthamendmentsummaries.com/ (08/02/2012)

προσωπική ελευθερία του ατόμου επιτρέποντας την παρέμβαση στη ζωή, την ελευθερία και την ιδιοκτησία μόνο μέσω του νόμου.⁷⁴

3.1.2 Ο νόμος για την ιδιωτική ζωή Privacy Act

Το privacy act θεσπίζει διαδικαστικά και ουσιαστικά δικαιώματα όσον αφορά τα προσωπικά δεδομένα.⁷⁵ Αυτά είναι:

- Το άτομο καθορίζει ποιες πληροφορίες που το αφορούν μπορούν να αρχειοθετηθούν
- Το άτομο έχει δικαίωμα πρόσβασης στις πληροφορίες
- Οι αρχές οφείλουν να χρησιμοποιήσουν της προσωπικές του πληροφορίες μόνο για νομοθετικά προσδιορισμένους σκοπούς
- Οι αρχές οφείλουν να προβαίνουν στην επεξεργασία των πληροφοριών αποκλειστικά και μόνο για το σκοπό για τον οποίο έχουν συλλεχθεί
- Η επίκληση του νόμου δεν είναι δυνατή, όταν πρόκειται για προστασία σπουδαίων δημοσίων συμφερόντων
- Επιτρέπει στα άτομα να ενάγουν την κυβέρνηση σε περίπτωση παραβίασης των διατάξεών του και να αξιωθούν αποζημίωση

Στα πλαίσια της συλλογής προσωπικών δεδομένων η διοίκηση είναι υποχρεωμένη να αντλεί τις πληροφορίες, όταν αυτό είναι δυνατόν, από το ίδιο το άτομο ιδιαιτέρως όταν πρόκειται να ληφθεί για αυτόν δυσμενής απόφαση, έτσι αποφεύγεται η χρήση πληροφοριών, χωρίς το άτομο που αφορούν οι πληροφορίες να το γνωρίζει, αν και η προστασία αυτή συχνά είναι ανεπαρκής διότι η διοίκηση έχει μεγάλο εύρος συλλογής πληροφοριών και το άτομο δεν έχει τη δυνατότητα να πληροφορηθεί τις πηγές της

⁷⁴ E. Chemerinsky, Constitutional law: principles and policies, 1997, σελ.638-642.

⁷⁵ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.149-150.

διοίκησης. Η διοίκηση μπορεί να συγκεντρώσει ελάχιστες πληροφορίες που είναι απαραίτητες για την εκπλήρωση της αποστολής της, ενώ αν οι πληροφορίες αυτές επηρεάζουν αρνητικά το άτομο, η υπηρεσία οφείλει να αναφέρει τον κανόνα δικαίου σύμφωνα με τον οποίο θεμελιώνεται η υποχρέωση του ατόμου για παροχή πληροφοριών, να του κοινοποιήσει τη νομική βάση, τον τρόπο χρήσης των πληροφοριών, και τις συνέπειες που μπορεί να έχει για το άτομο η μη παροχή των πληροφοριών αυτών.⁷⁶

Σύμφωνα με το νόμο, τα άτομα έχουν το δικαίωμα της πρόσβασης και της διόρθωσης, επιτρέπεται ωστόσο σε ένα άτομο η πρόσβαση μόνον εφόσον τα δεδομένα του τηρούνται από την υπηρεσία στο πλαίσιο ενός "συστήματος καταχώρισης", όταν δηλαδή αναζητούνται με το όνομα του αιτούντος ή με έναν κωδικό. Το "σύστημα καταχώρισης δεδομένων" περιέχει εξατομικευμένες πληροφορίες προσωπικού χαρακτήρα για μεμονωμένα άτομα. Υπηρεσίες όπως ομοσπονδιακά περιφερειακά δικαστήρια, πολιτειακές υπηρεσίες και νομικά πρόσωπα ιδιωτικού δικαίου δεν υπόκεινται στο νόμο.

Στην υπόθεση Clarkson κατά της Φορολογικής Υπηρεσίας (I.R.S.), 678 F.2d 1368 (11ο Cir. 1982),⁷⁷ ο ενάγων, ένας διαδηλωτής, ερευνήθηκε από την Φορολογική Υπηρεσία (I.R.S.), η οποία κράτησε ένα αρχείο με εκθέσεις επιτήρησης, ενημερωτικά δελτία, και δελτία τύπου. Το δικαστήριο έκρινε ότι αυτά ήταν κατά παράβαση του νόμου περί προστασίας προσωπικών δεδομένων, ακόμη και όταν η IRS υποστήριξε ότι τα αρχεία δεν βρίσκονταν σε ένα "σύστημα αρχείων", αφού κρατήθηκαν σε ένα γενικό "Αρχείο Διαμαρτυρίας φόρου", από το οποίο η IRS είπε δεν θα μπορούσε να ανακτήσει μεμονωμένες εγγραφές, από το όνομα ή από τον κωδικό.

Το δικαίωμα της διόρθωσης προβλέπει ότι σε περίπτωση που ο ενδιαφερόμενος πολίτης δεν συμφωνεί με το περιεχόμενο των προσωπικών του πληροφοριών μπορεί να ζητήσει τη διόρθωση τους, αυτό γίνεται γραπτά ή και προφορικά. Αν η διοίκηση δεν ανταποκρίνεται στο αίτημα του πολίτη τότε προβλέπεται η δυνατότητα υποβολής

⁷⁶ www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dt/830/830120/830120el.pdf (08/02/2012)

⁷⁷ www.epic.org/privacy/1974act/ (08/02/2012)

έκθεσης, στην οποία το άτομο καταγράφει τους λόγους για τους οποίους αμφισβητεί τις πληροφορίες αυτές. Από την πλευρά της η διοίκηση, πρέπει να χαρακτηρίσει τα στοιχεία αυτά και σε κάθε κοινοποίηση να επισυνάπτει την έκθεση του πολίτη, μπορεί επίσης να εκφράσει και την δική της θέση και να αναφέρει τους λόγους για τους οποίους δεν έκανε δεκτό το αίτημα του ατόμου, η έκθεση αυτή θα επισυνάπτει κάθε κοινοποίηση των πληροφοριών του ατόμου.

Η δεύτερη παράγραφος του νόμου περιορίζει το δικαίωμα μιας υπηρεσίας να κοινοποιήσει πληροφορίες εκτός αν πληρούν μια από τις δώδεκα προϋποθέσεις⁷⁸ που προβλέπει ο νόμος, αυτές αφορούν:

- στελέχη και υπαλλήλους του οργανισμού που διατηρούν αρχεία που έχουν ανάγκη για την τέλεση των καθηκόντων τους
- σκοπούς που απαιτούνε από το άρθρο 552
- χρήσης ρουτίνας, δηλαδή όταν το αρχείο έχει συλλεγεί για το σκοπό αυτό
- λόγους απογράφης ή συναφής δραστηριότητες
- έναν παραλήπτη ο οποίος έδωσε στον οργανισμό γραπτή επιβεβαίωση ότι η καταγραφή θα χρησιμοποιηθεί ως απλά μια στατιστική έρευνα και τα αρχεία θα μεταφερθούν σε μια μορφή που δεν θα είναι αναγνωρίσιμα
- ένα αρχείο που έχει ιστορική ή άλλη αξία που να δικαιολογεί την φύλαξη του από την κυβέρνηση των Η.Π.Α.
- μια άλλη υπηρεσία των Η.Π.Α. για την επιβολή του νόμου σε μια εγκληματική δραστηριότητα
- όταν επηρεάζεται η υγεία και η ασφάλεια ενός ατόμου
- για σκοπούς του Κογκρέσου

⁷⁸ www.law.cornell.edu/uscode/text/5/552a&usg=ALkJrhiUJhA16pMDtQR1H_YUsJdYMQxRIQ (08/02/2012)

- για τον Γενικό Ελεγκτή ή οποιονδήποτε εξουσιοδοτημένο εκπρόσωπο του, κατά τη διάρκεια άσκησης των καθηκόντων του
- για κάθε αρμόδιο δικαστήριο
- για γραφείο πληροφόρησης των καταναλωτών

Η διοίκηση οφείλει να συλλέξει και να καταχωρίσει εκείνες και μόνο τις πληροφορίες που χρειάζεται για την εκπλήρωση του σκοπού που γίνεται η συλλογή. Το περιεχόμενο των πληροφοριών που συλλέγονται προσδιορίζεται από τα καθήκοντα της εκάστοτε υπηρεσίας που κάνει τη συλλογή. Οι πληροφορίες αυτές θα πρέπει να είναι ακριβείς και επίκαιρες, τα στοιχεία τα οποία στην πορεία της ιστορικής εξέλιξης έχουν καταστεί ασήμαντα πρέπει να διαγραφούν, καθώς η διοίκηση έχει υποχρέωση να ελέγχει για την επικαιρότητα των πληροφοριών. Στην πραγματικότητα αυτό δεν σημαίνει πως η διοίκηση πριν από κάθε χρήση των πληροφοριών πρέπει να ελέγξει αν είναι ορθές ή όχι γιατί αυτό εικάζεται εφόσον δεν συντρέχει λόγος αμφισβήτησης.⁷⁹

Σύμφωνα με την τρίτη προϋπόθεση <<για χρήσης ρουτίνας >> ή <<συνήθης χρήση >> παρακάμπτεται ο περιορισμός για την κοινοποίηση πληροφοριών εφόσον οι πληροφορίες έχουν συλλεγεί για το σκοπό για τον οποίο χρησιμοποιούνται, και δημοσιεύονται στο ομοσπονδιακό μητρώο, δημιουργώντας προβλήματα όταν αντιπαρατίθενται με την αρχή της δέσμευσης και της εξειδίκευσης του σκοπού. Τα δικαστήρια αρκούνται στη δημοσίευση της διοικητικής διάταξης και δεν ελέγχουν αν ο σκοπός για τον οποίο έχουν συγκεντρωθεί οι πληροφορίες είναι ίδιος με αυτόν για τον οποίο χρησιμοποιούνται. Επίσης όταν η διοικητική αρχή προτίθεται να χρησιμοποιήσει ήδη αποθηκευμένες πληροφορίες οφείλει να κοινοποιήσει τη χρήση στο άτομο 30 μέρες πριν από τη δημοσίευση, ώστε το άτομο να έχει τη δυνατότητα αντιμετώπισης και μετά να δημοσιευθεί στο ομοσπονδιακό μητρώο.⁸⁰

⁷⁹ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.151

⁸⁰ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.153

Στην υπόθεση Britt κατά Ναυτικής υπηρεσίας ερευνών, 886 F.2d 544 (3d Cir. 1989), Ελεγκτικές Υπηρεσίες Ναυτικού (NAK) ερευνούσαν τον κ. Britt. Υπάλληλο της Υπηρεσίας Μετανάστευσης και Πολιτογράφησης (INS) για ανάρμοστες κατασχέσεις⁸¹. Η NAK κυκλοφόρησε προκαταρκτικές έρευνες τους για το INS. Ο κ. Britt. μήνυσε για ανάρμοστη γνωστοποίηση σύμφωνα με το νόμο περί προστασίας προσωπικών δεδομένων. Η NAK υποστήριξε ότι η δημοσιοποίησή τους από την έρευνα εμπίπτει στη "συνήθη χρήση" που είναι εξαίρεση, αφού η χρήση ρουτίνας δημοσιεύεται στο ομοσπονδιακό μητρώο. Δεδομένου ότι το INS είναι μια ομοσπονδιακή ρυθμιστική αρχή σε μια ερευνητική μονάδα, η NAK ισχυρίστηκε ότι αυτό ήταν μια χρήση ρουτίνας, που κανονικά δημοσιεύεται στο ομοσπονδιακό μητρώο, και ως εκ τούτου δεν υπόκειται στο νόμο περί ιδιωτικής ζωής. Το τρίτο εφετείο διαφώνησε, λέγοντας ότι το εύρος της ρήτρας που επικαλείται δεν παρέχει επαρκή προειδοποίηση για τα άτομα και τις πληροφορίες που τους αφορούν.

Όταν οι πληροφορίες χρησιμοποιούνται για στατιστικούς σκοπούς ο αποδέκτης των πληροφοριών αυτών διαβεβαιώνει γραπτώς ότι οι πληροφορίες χρησιμοποιούνται για καθαρά και μόνο στατιστικούς σκοπούς και ότι μετά από αυτό ανωνυμοποιούνται. Η κοινοποίηση των πληροφοριών αυτών προσβάλλει το δικαίωμα της αυτοδιάθεσης των πληροφοριών γιατί δεν είναι εύκολο η διοίκηση να ελέγξει αν ο αποδεκτής τηρεί τους όρους της διαβεβαίωσης.

Ως "άτομα" νοούνται οι πολίτες των Ηνωμένων Πολιτειών ή αλλοδαποί που διαθέτουν νόμιμη κατοικία, επισκέπτες ή αλλοδαποί εξαιρούνται. Τον Ιανουάριο του 2009, η πολιτική της Υπηρεσίας Εσωτερικής Ασφάλειας τροποποιήθηκε με αποτέλεσμα κάθε δεδομένο προσωπικού χαρακτήρα που συλλέγεται και χρησιμοποιείται να αντιμετωπίζεται ως ένα σύστημα καταχώρισης δεδομένων υποκειμένο στο νόμο για την ιδιωτική ζωή, ανεξαρτήτως του εάν η πληροφορία αφορά πολίτες των ΗΠΑ, μόνιμο κάτοικο με νόμιμη άδεια, επισκέπτη ή αλλοδαπό. Μη Αμερικάνοι πολίτες έχουν δικαίωμα πρόσβασης σε πληροφορίες που τους αφορούν και δικαίωμα διόρθωσής τους με την επιφύλαξη εξαιρέσεων σύμφωνα με το νόμο περί ιδιωτικής ζωής, αλλά δεν θεσπίζεται δικαίωμα δικαστικής προσφυγής για αυτούς. Επιπλέον, τα δεδομένα

⁸¹ www.epic.org/privacy/1974act/ (08/02/2012)

προσωπικού χαρακτήρα μη Αμερικανών πολιτών που δεν τηρούνται σε μεικτά συστήματα, αλλά σε συστήματα που αφορούν μόνο αλλοδαπούς (όπως το ηλεκτρονικό σύστημα παροχής άδειας ταξιδιού των ΗΠΑ-ESTA)⁸² δεν προστατεύονται και δεν καλύπτονται από την πολιτική αυτή.

3.1.3 Νόμοι των Η.Π.Α. σε σχέση με την προστασία προσωπικών δεδομένων

Ο νόμος fair credit reporting act για την πιστοληπτική ικανότητα ρυθμίζει τη χρήση πληροφοριών που συλλέγονται από εταιρείες πιστοληπτικού ελέγχου. Ο fair credit reporting act αναφέρεται αποκλειστικά στους φορείς παροχής οικονομικών πληροφοριών⁸³ και ρυθμίζει τη δημοσιοποίηση και μεταβίβαση προσωπικών δεδομένων και όχι την συλλογή αυτών, έτσι δεν προβλέπει περιορισμούς στον τρόπο και την έκταση των σελλεχθέντων πληροφοριών. Επίσης δεν προβλέπεται η ενημέρωση και η συγκατάθεση του καταναλωτή για την συλλογή των δεδομένων. Τα δεδομένα αυτά μπορούν να μετεβιβασθούν σε τρίτους όταν ο καταναλωτής επιτρέπει την μετάδοση, ή όταν ο τρίτος που θα λάβει τα δεδομένα σκοπεύει να τα χρησιμοποιήσει για τη χορήγηση μιας πίστωσης, μιας εργασιακής σχέσης, για τη χορήγηση μιας άδειας, ή οικονομικής βοήθειας και συντρέχει δικαιολογημένη ανάγκη για τη γνώση των δεδομένων αυτών. Αν συντρέχει ένας επιτρεπτός σκοπός για την πρώτη χρήση των δεδομένων δεν προβλέπονται περιορισμοί για την περαιτέρω χρήση αυτών των δεδομένων. Κάθε καταναλωτής έχει το δικαίωμα πρόσβασης στα στοιχεία που έχουν

⁸² Από τις 12 Ιανουαρίου 2009, όλα τα άτομα που ταξιδεύουν στις Ηνωμένες Πολιτείες στα πλαίσια του Προγράμματος Απαλλαγής από Βίζα (VWP) απαιτείται να έχουν μια ταξιδιωτική άδεια πριν ξεκινήσουν το ταξίδι τους. Το ESTA είναι διαθέσιμο με τη πληρωμή ενός μικρού ποσού (\$14). www.athens.usembassy.gov/faq-gr.html (08/02/2012)

⁸³ Σύμφωνα με το 15 U.S.C.A. παρ.1681α (f) φορέας παροχής οικονομικών πληροφοριών θεωρείται όποιος έναντι χρηματικής αμοιβής ή με βάση συμφωνίας αμοιβαιότητας συλλέγει πληροφορίες για τους καταναλωτές ή πληροφορίες για την πιστωτική φερεγγυότητα τους με σκοπό τον έλεγχο (Customer Report) και τη μεταβίβαση τους σε τρίτους

συλλεγεί, επειδή όμως οι σχετικές διατάξεις δεν προβλέπουν την υποχρέωση των φορέων για την ενημέρωση του καταναλωτή δεν ικανοποιείται στην πράξη το δικαίωμα αυτό. Ο νόμος δεν προβλέπει περιορισμούς στην αποθήκευση και τη διάρκεια αυτής, απαγορεύει όμως την μετάδοση συγκεκριμένων πληροφοριών μετά την πάροδο εύλογου χρονικού διαστήματος. Η εφαρμογή του νόμου ελέγχεται από την Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission).

Ο νόμος Electronic Communications Privacy Act 1986 έχει ως αντικείμενο την προστασία του λόγου όταν αυτός μεταφέρεται μέσα από τεχνικές εγκαταστάσεις από παράνομη υποκλοπή και καταγραφή, αποσκοπεί στην προστασία του ατόμου από κρατικές επεμβάσεις αλλά και από προσβολές που προέρχονται από τρίτους. Το περιεχόμενο των ιδιωτικών συνομιλιών προστατεύεται από την υποκλοπή και την καταγραφή και η παραβίαση αυτών δίνει το δικαίωμα στον ενδιαφερόμενο να ασκήσει αγωγή αποζημίωσης, ακόμη και φυλάκισης. Το περιεχόμενο αυτών των συνομιλιών μπορεί να γνωστοποιηθεί όταν ο αποστολέας ή ο αποδεκτής έχουν δώσει τη συναίνεση τους.

Ο νόμος Cable Communication Policy Act 1984 για της καλωδιακές επικοινωνίες, αναφέρεται στις συνήθειες των συνδρομητών σταθερής τηλεφωνίας. Οι συνδρομητές θα πρέπει το αργότερο μετά από ένα χρόνο από την υπογραφή της σύμβασης να ενημερώνονται για το ποια δεδομένα από αυτά που είναι ικανά για την αναγνώριση της ταυτότητας τους έχουν συλλεγεί, τον σκοπό που εξυπηρετούν, αν έχουν μεταδοθεί σε τρίτους, την διάρκεια της αποθήκευσης, το δικαίωμα πρόσβασης στα δεδομένα και της νομικές δυνατότητες για την τήρηση των περιορισμών. Οι συνδρομητές έχουν το δικαίωμα της διόρθωσης των λανθασμένων δεδομένων ενώ η επιχείρηση πρέπει να καταστρέφει τα δεδομένα που δεν είναι πλέον αναγκαία για την επίτευξη του αρχικού σκοπού συλλογής. Τα στοιχεία μπορούν να μεταδοθούν μόνο με τη συναίνεση του συνδρομητή ή για επιχειρηματικούς λόγους ή εφόσον έχει διαταχθεί δικαστικά.⁸⁴

Ο νόμος Computer Matching Act 1988 απαγορεύει την μετάδοση πληροφοριών που αφορούν προσωπικά δεδομένα και την σύγκριση αυτών, εφόσον δεν υπάρχει

⁸⁴ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.165.

γραπτή συμφωνία μεταξύ των ενδιαφερομένων ομοσπονδιακών αρχών. Η μετάδοση αυτή θα πρέπει να δημοσιευθεί στο ομοσπονδιακό μητρώο και αφού πρόκειται για συλλογή προσωπικών δεδομένων, οι διοικητικές αρχές είναι υποχρεωμένες να ενημερώσουν τον πολίτη για τη συλλογή των δεδομένων. Ο νόμος επίσης προβλέπει το << Data Integrity Boards>> που έχει ως σκοπό τον έλεγχο της ορθότητας των δεδομένων, ώστε να επιτευχθεί η μέγιστη αξία της χρήσης τους.

Ο νόμος Computer Security Act αναθέτει σε ένα τμήμα του υπουργείου Εμπορίας την ευθύνη για την δημιουργία διατάξεων με σκοπό την προστασία των ευαίσθητων δεδομένων. Η εκτελεστική εξουσία έχει τη δυνατότητα να τροποποιεί τα μέτρα που προβλέπονται για την προστασία των προσωπικών δεδομένων, έτσι ο πολίτης δεν έχει το δικαίωμα να επηρεάζει και να καθορίζει τη χρήση των προσωπικών του δεδομένων και η εκτελεστική εξουσία έχει απεριόριστες αρμοδιότητες. Σύμφωνα με τον Σ. Σημίτη, με το νόμο αυτό ανατρέπεται η πληροφοριακή ισορροπία μεταξύ νομοθετικής και εκτελεστικής εξουσίας.⁸⁵

3.1.4 Αυτορύθμιση σε δημόσιο και ιδιωτικό τομέα

Στις Η.Π.Α. ακολουθείται μια φιλελεύθερη προσέγγιση που επιτρέπει την αυτορύθμιση σε κάθε κλάδο, δίνοντας έτσι τη δυνατότητα σε φορείς και επιχειρήσεις να δρουν κατά βούληση, και να χρησιμοποιούν δικό τους πλαίσιο κανόνων. Ενδεικτικά θα αναφέρουμε παρακάτω κάποιες από τις κρατικές πρωτοβουλίες.⁸⁶

⁸⁵ Σ. Σημίτης, Ηλεκτρονικοί υπολογιστές και νομική παιδεία. Προϋποθέσεις, επιπτώσεις, προοπτικές, Πληροφορική και δίκαιο, 1987, σελ.75.

⁸⁶ Γ. Γιαννόπουλος, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002, σελ.96-97.

Η ομάδα Information Infrastructure Task Force συστάθηκε επί προεδρίας Κλίντον και δημοσίευσε το έγγραφο Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information,⁸⁷ που διατυπώνει γενικές αρχές σύμφωνα με αυτές του Ο.Ο.Σ.Α., και αναφέρονται ως πρότυπο σε αρκετές ιστοσελίδες δημοσιών υπηρεσιών των Η.Π.Α.

Τον Οκτώβριο του 1995 η Ρυθμιστική Αρχή Τηλεπικοινωνιών και Πληροφοριών (National Telecommunication and Information Administration) δημοσίευσε το έγγραφο Privacy and the National Information Infrastructure: Safeguarding Telecommunication-Related Personal Information,⁸⁸ το οποίο προτείνει στους παρόχους υπηρεσιών πληροφόρησης και τηλεπικοινωνιών να ενημερώνουν τους χρήστες για την πολιτική τους όσον αφορά τα προσωπικά δεδομένα, και να εξασφαλίζουν την συγκατάθεση τους όσον αφορά τη χρήση των πληροφοριών που τους αφορούν. Το 1998 η ίδια επιτροπή εξέδωσε το Elements Self-Regulation for Protection of Privacy, το οποίο περιγράφει τις ενέργειες τις οποίες πρέπει να προβεί ο ιδιωτικός τομέας ώστε να επιτευχθεί ικανοποιητικό επίπεδο προστασίας προσωπικών δεδομένων.

Το Δεκέμβριο του 1997 η Ομοσπονδιακή Επιτροπή Εμπορίου εξέδωσε έγγραφο Individual Reference Services: A Report to Congress,⁸⁹ με το οποίο περιγράφει τους κινδύνους από τη χρήση συνδυασμένων βάσεων δεδομένων, και σχολιάζει κώδικες δεοντολογίας του ιδιωτικού τομέα. Το 1998 εξέδωσε έκθεση προς το Κογκρέσο (Privacy Online: a Report to Congress) στην οποία διατυπώνει ότι πολύ λίγες ιστοσελίδες τηρούν τις γενικές αρχές προστασίας προσωπικών δεδομένων. Σε δεύτερη έκθεση το 1999 Self-regulation and Privacy Online καλεί τους φορείς να λάβουν περισσότερα μέτρα για την εφαρμογή των αρχών, ενώ το 2000 εξέδωσε τρίτη έκθεση Privacy Online: Fair Information Practices in the Electronic Marketplace, στην οποία αναφέρει αποτελέσματα σχετικής έρευνας που δείχνουν ότι υπάρχει βελτίωση

⁸⁷ www.aspe.hhs.gov/datacncl/niiprivp.htm (08/02/2012)

⁸⁸ www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html (08/02/2012)

⁸⁹ www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (08/02/2012)

εκφράζοντας όμως επιφυλάξεις για την πλήρη αποτελεσματικότητα των πρωτοβουλιών αυτών, και παροτρύνει το Κογκρέσο να προβεί σε νομοθετικές ρυθμίσεις.⁹⁰

Στον ιδιωτικό τομέα, αρκετοί οργανισμοί και ενώσεις έχουν δημοσιεύσει σχετικές οδηγίες και κώδικες δεοντολογίας προς τα μέλη τους:

- Ο Οργανισμός Πιστοληπτικής Ικανότητας⁹¹ (Individual Reference Services Group) το 1997 υιοθέτησε τις σχετικές οδηγίες της Ομοσπονδιακής Επιτροπής Εμπορίου (F.T.C.) για τη χρήση συνδυασμένων βάσεων δεδομένων. Τα μέλη του οργανισμού υποβάλλονται εθελοντικά σε ετήσιο έλεγχο από ανεξάρτητο ελεγκτή.
- Η ένωση Online Privacy Alliance το 1998 δημοσίευσε οδηγίες με τις οποίες συστήνει στα μέλη της να ακολουθούν της αρχές του Ο.Ο.Σ.Α. και να χρησιμοποιούν ειδικό λογισμικό για την προστασία των ανηλίκων.⁹²
- Το 1999 η Ένωση Εμπορικής Προώθησης (Direct Marketing Association) και η Ένωση American Electronics Association δημοσίευσαν γενικές αρχές προστασίας προσωπικών δεδομένων που όλα τα μέλη πρέπει να τις τηρούν.⁹³
- Το 2001 το Συμβούλιο πληροφορικής (Information Technology Industry Council)⁹⁴ δημοσίευσε αρχές με βάση της οποίες τα μέλη μπορούν να καθορίσουν τη δική τους πολιτική προστασίας προσωπικών δεδομένων.
- Το σύστημα πιστοποίησης Better Business Bureau αποδίδει στα μέλη του, εφόσον πληρούν συγκεκριμένες προδιαγραφές, το ειδικό σήμα <<BBBonline>> το οποίο προβλέπει ειδικές διαδικασίες γονικής συναίνεσης, όταν συγκεντρώνονται πληροφορίες από ανηλίκους χρήστες.

⁹⁰ www.ftc.gov/reports/privacy2000/privacy2000.pdf (08/02/2012)

⁹¹ www.ntia.doc.gov/legacy/ntiahome/privacy/mail/disk/irsgcom.html (08/02/2012)

⁹² www.privacyalliance.org/ (08/02/2012)

⁹³ www.thedma.org/services/privacy/ (08/02/2012)

⁹⁴ www.itic.org (08/02/2012)

3.1.5 Διευθέτηση <<ασφαλούς λιμένα >> (safe harbor)

Σύμφωνα με την τέταρτη Ετήσια Έκθεση της Ομάδας Εργασίας για την προστασία δεδομένων το 2001, ο συνδυασμός των ανωτέρω μέτρων δεν είναι αρκετά αξιόπιστος ώστε να παρέχει κατάλληλη προστασία σε όλες τις περιπτώσεις διαβίβασης προσωπικών δεδομένων από την Ευρωπαϊκή Ένωση. Για το λόγο αυτό ακολούθησε σειρά διαβουλεύσεων ανάμεσα στην Ευρωπαϊκή Ένωση και τις Η.Π.Α. που κατέληξαν στην διευθέτηση <<ασφαλούς λιμένα>>.⁹⁵ Με διευθέτηση αυτή το Υπουργείο Εμπορίας των Η.Π.Α. έχει την υποχρέωση να διατηρεί καταλόγους με τις εταιρίες οι οποίες τηρούν ένα ελάχιστο σύνολο κανόνων προστασίας δεδομένων και αντίστοιχους μηχανισμούς ελέγχου. Έτσι οι Ευρωπαϊκές εταιρίες μπορούν να πραγματοποιήσουν ελεύθερα συναλλαγές με εταιρίες των Η.Π.Α. οι οποίες έχουν προσχωρήσει στους καταλόγους του <<ασφαλούς λιμένα>>.

Οι οργανισμοί πρέπει να συμμορφώνονται με τις επτά αρχές⁹⁶ του ασφαλούς λιμένα, οι οποίες απαιτούν τα εξής:

- Ειδοποίηση: Οι οργανισμοί θα πρέπει να ενημερώνουν τους ενδιαφερομένους για τους σκοπούς για τους οποίους συλλέγονται και χρησιμοποιούνται οι πληροφορίες σχετικά με αυτούς. Θα πρέπει να παρέχουν πληροφορίες σχετικά με το πώς τα άτομα μπορούν να επικοινωνήσουν με την οργάνωση, με οποιοσδήποτε απορίες ή παράπονα, τα είδη των τρίτων στους οποίους γνωστοποιεί τις πληροφορίες, και τις επιλογές και τα μέσα που διαθέτει ο οργανισμός για τον περιορισμό της χρήσης και της αποκάλυψή τους.
- Επιλογή: Οι οργανισμοί πρέπει να παρέχουν στα άτομα τη δυνατότητα να επιλέξουν ποια προσωπικά στοιχεία τους θα γνωστοποιούνται σε τρίτους, ή θα χρησιμοποιηθούν για σκοπούς ασύμβατους με το σκοπό για τον οποίο συλλέχθηκαν αρχικά.

⁹⁵ www.export.gov/safeharbor (08/02/2012)

⁹⁶ www.export.gov/safeharbor/eu/eg_main_018476.asp (08/02/2012)

- **Μεταβίβαση:** Όταν ένας οργανισμός επιθυμεί να μεταφέρει πληροφορίες σε ένα τρίτο μέρος το οποίο ενεργεί ως πράκτορας, μπορεί να το πράξει εάν εξασφαλίζει ότι ο τρίτος συμφωνεί με τις αρχές του ασφαλούς λιμένα και της προστασίας προσωπικών δεδομένων, ή υπόκειται στην παρούσα οδηγία ή μια άλλη διαπίστωση επάρκειας. Ως εναλλακτική λύση, ο οργανισμός μπορεί να συνάψει γραπτή συμφωνία με τρίτο μέρος, σύμφωνα με την οποία, ο τρίτος παρέχει τουλάχιστον το ίδιο επίπεδο προστασίας της ιδιωτικής ζωής, όπως απαιτείται από τις αρμόδιες αρχές.
- **Πρόσβαση:** Τα άτομα πρέπει να έχουν πρόσβαση στις προσωπικές πληροφορίες που κατέχει για 'αυτούς ένας οργανισμός και να είναι σε θέση να διορθώσουν, να τροποποιήσουν, ή να διαγράψουν τις πληροφορίες που είναι ανακριβείς.
- **Ασφάλεια:** Οι οργανώσεις πρέπει να λαμβάνουν εύλογες προφυλάξεις για την προστασία των προσωπικών πληροφοριών από απώλεια, κακή χρήση και μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, τροποποίηση και καταστροφή.
- **Η ακεραιότητα των δεδομένων:** Οι προσωπικές πληροφορίες πρέπει να είναι σχετικές με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν. Ένας οργανισμός πρέπει να λαμβάνει εύλογα μέτρα για να εξασφαλίσει ότι τα δεδομένα είναι αξιόπιστα για την προοριζόμενη χρήση του, είναι ακριβή, πλήρη και ενημερωμένα.
- **Επιβολή:** Προκειμένου να εξασφαλιστεί η συμμόρφωση με τις αρχές του ασφαλούς λιμένα, πρέπει να υπάρχουν άμεσα διαθέσιμοι και προσιτοί ανεξάρτητοι μηχανισμοί προσφυγής, ώστε να μπορούν να διερευνηθούν παράπονα και διαφορές του κάθε ατόμου και να επιλυθούν. Να έχουν εφαρμοστεί οι διαδικασίες για την επαλήθευση, ότι οι εταιρείες τηρούν τις αρχές του ασφαλούς λιμένα και τις υποχρεώσεις για την αντιμετώπιση προβλημάτων, που προκύπτουν από τη μη συμμόρφωση με τις αρχές. Οι κυρώσεις πρέπει να είναι αρκετά αυστηρές για να εξασφαλιστεί η συμμόρφωση. Οι οργανισμοί που αποτυγχάνουν να παρέχουν ετήσιες επιστολές πιστοποίησης δεν θα εμφανίζονται πλέον στη λίστα των συμμετεχόντων και δεν θα είναι πλέον εξασφαλισμένες.

Η διευθέτηση <<ασφαλούς λιμένα>> λειτουργεί από την 1^η Νοεμβρίου 2000, οπότε τέθηκε στη διάθεση των εταιριών ειδική ιστοσελίδα στην οποία μπορούν οι ίδιες

να δηλώσουν τα στοιχεία τους ώστε να δηλώσουν συμμετοχή στο πρόγραμμα, μια διαδικασία αυτοπιστοποίησης που επικουρείται από την Αμερικάνικη νομοθεσία αλλά η συμμετοχή είναι εθελοντική.⁹⁷

3.2. Γερμανία [ΑΙΛΕΣ]

Η Δυτική Γερμανία ήταν η πρώτη χώρα που ρύθμισε νομοθετικά το πρόβλημα της προστασίας του πολίτη από τη λειτουργία των πληροφοριακών συστημάτων. Στις 7 Οκτωβρίου του 1970, η Γερμανική Πολιτεία της Έσσης ψήφισε τον πρώτο νόμο σε ευρωπαϊκό επίπεδο που καθιέρωσε τον όρο <<προσωπικά δεδομένα>>. Ο καθηγητής Σπύρος Σημίτης, σχολιάζοντας το νόμο της Έσσης, παρατηρεί ότι είναι: <<η πρώτη νομοθετική αντίδραση στην επιθυμία να προστατευθεί το άτομο κατά των ενδεχομένων επιπτώσεων της χρήσης των ηλεκτρονικών υπολογιστών από τη Δημόσια Διοίκηση>>.⁹⁸ Το 1977 ψηφίστηκε από την Ομοσπονδιακή Δημοκρατία της Γερμανίας ο νόμος (Bundesdatenschutzgesetz ή BDSG) περί προστασίας εναντίον της καταχρήσεως των προσωπικών δεδομένων κατά την επεξεργασία αυτών, που ισχύει από την 1η Ιανουαρίου 1978, όπως έχει ήδη τροποποιηθεί. Η νομοθεσία συμπληρώνεται από ένα πλέγμα σχετικών διατάξεων⁹⁹ που αφορούν ειδικά στα μέσα ενημέρωσης, τον τομέα των τηλεπικοινωνιών και εξ' αποστάσεως υπηρεσιών.

⁹⁷ Γ. Γιαννόπουλος, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002, σελ.102.

⁹⁸ Αναστάσιος Μαρίνος, Ηλεκτρονικοί υπολογιστές και το δίκαιο: informatique juridique, 1980, σελ.85.

⁹⁹ www.bfd.bund.de/information/gesetze.html (09/02/2012)

3.2.1 Το Σύνταγμα, της Γερμανίας (Grundgesetz)

Το Σύνταγμα, της Γερμανίας (Grundgesetz) δεν δημιουργεί ένα ειδικό δικαίωμα στην ιδιωτική ζωή, τα συμφέροντα της ιδιωτικής ζωής προστατεύονται μέσω τεσσάρων συνταγματικών διατάξεων. Αυτές είναι: α) το απαραβίαστο της ανθρώπινης αξιοπρέπειας κατά το άρθρο 1 του Συντάγματος, β) το δικαίωμα στην προσωπικότητα σύμφωνα με το άρθρο 2 (1), γ) η προστασία των γραμμάτων, των μηνυμάτων και των τηλεπικοινωνιών σύμφωνα με το άρθρο 10. και δ) η εγγύηση του απαραβίαστου του σπιτιού κάτω από Άρθρο 13.¹⁰⁰ Στο επίκεντρο της συνταγματικής τάξης βρίσκεται η αξία και η αξιοπρέπεια του προσώπου, το οποίο λειτουργεί ως μέλος μιας ελεύθερης κοινωνίας. Η προστασία του κατοχυρώνεται με το δικαίωμα της προσωπικότητας από το σύνταγμα, το οποίο αποκτά ιδιαίτερη σημασία ενόψει της σύγχρονης ανάπτυξης της τεχνολογίας και τον κινδύνων που μπορεί να επιφέρει η ανάπτυξη αυτή στην προσωπικότητα του ατόμου.¹⁰¹

Το άρθρο 1 του Συντάγματος δηλώνει ότι: << Η ανθρώπινη αξιοπρέπεια είναι απαραβίαστη. Είναι καθήκον της κρατικής εξουσίας ο σεβασμός και η προστασία της>>. Το κράτος έχει υποχρέωση να δημιουργήσει τις προϋποθέσεις που ευνοούν και διαφυλάτουν τα ανθρώπινα δικαιώματα και το άτομο δεν θα πρέπει να είναι ένα «απλό αντικείμενο» της πολιτείας. Η προστασία της ανθρώπινης αξιοπρέπειας είναι το πιο σημαντικό από όλα τα βασικά δικαιώματα και το άρθρο 1 του Συντάγματος δεν μπορεί να τροποποιηθεί ή να διαγραφεί.

Το άρθρο 2 (1) ορίζει ότι << Κάθε πρόσωπο έχει το δικαίωμα στην ελεύθερη ανάπτυξη της προσωπικότητάς του, εφόσον αυτό δεν παραβιάζει τα δικαιώματα των άλλων ή προσβάλλει τη συνταγματική τάξη ή τον ηθικό νόμο>>. Το άρθρο 2 (1) έχει ερμηνευθεί ως εγγύηση για μια γενική ελευθερία δράσης, και σε συνδυασμό με το

¹⁰⁰ Σύνταγμα Γερμανίας, Grundgesetz [Basic Law] αρθ.1,2,10,13 www.iuscomp.org/gla/statutes/GG.htm (09/02/2012)

¹⁰¹ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.137.

άρθρο 1, ως γενικό δικαίωμα στην προσωπικότητα. Το δικαίωμα της προσωπικότητας περιλαμβάνει επίσης το δικαίωμα να «πληροφοριακής αυτοδιάθεσης», το οποίο δίνει στο άτομο το δικαίωμα να ελέγχει το πότε και κάτω από ποιες συνθήκες τα δεδομένα προσωπικού χαρακτήρα θα δημοσιευθούν. Το 1983 σε υπόθεση κατά του νόμου απογραφής της κυβέρνησης, το Ομοσπονδιακό Συνταγματικό Δικαστήριο αναγνώρισε επίσημα "το δικαίωμα της πληροφοριακής αυτοδιάθεσης" ενός ατόμου, που περιορίζεται μόνο από το «κυρίαρχο δημόσιο συμφέρον».¹⁰²

Το άρθρο 10 προστατεύει το απόρρητο ορισμένων επικοινωνιών. Συγκεκριμένα, προστατεύει τα προσωπικά δεδομένα στο χώρο των ταχυδρομείων και των τηλεπικοινωνιών. Το άρθρο 10 δίνει ένα ατομικό έλεγχο για το πώς ταχυδρομικές επικοινωνίες αποθηκεύονται και χρησιμοποιούνται. Η προστασία των τηλεπικοινωνιών περιλαμβάνει τις τηλεφωνικές κλήσεις, καθώς και όλα τα άλλα ενσύρματα και ασύρματα μέσα επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο. Η πολιτεία μπορεί να άρει το δικαίωμα λαμβάνοντας έκτακτα μέτρα για την προστασία του Συντάγματος και της πολιτείας.

Το άρθρο 13 προστατεύει την ιδιωτικότητα του σπιτιού. Αυτή η βασική αρχή έχει ως στόχο να παρέχει έναν θεμελιώδες χώρο στον οποίο ένα άτομο έχει το δικαίωμα να αποσύρεται και να μένει μόνο του, να διατηρεί το δικαίωμα του κατοίκου να καθορίσει ποιος μπορεί να έχει πρόσβαση στο σπίτι του, καθώς και το πότε και υπό ποιες συνθήκες θα γίνει αυτό. Το απαραβίαστο της κατοικίας δεν εφαρμόζεται όταν ο κάτοικος συναινεί σε μια έρευνα, ή άλλη παραβίαση της ιδιωτικής ζωής του στο σπίτι. Η έννοια του σπιτιού έχει ερμηνευθεί ευρέως για να γίνει κατανοητή, περιλαμβάνει χώρους εργασίας, όπως τα γραφεία, αλλά και εξωτερικά μέρη του σπιτιού, όπως τις αυλές και τους κήπους. Το Ομοσπονδιακό Συνταγματικό Δικαστήριο της Γερμανίας έχει δώσει στους χώρους εργασίας, όπως τα γραφεία ένα πιο περιορισμένο επίπεδο προστασίας της ιδιωτικής ζωής, λόγω των ισχυρών κοινωνικών δεσμών που σχετίζονται με τους εν λόγω χώρους.

¹⁰² Ομοσπονδιακό Συνταγματικό Δικαστήριο (Bundesverfassungsgericht) ,15 December 1983, ΑΠ: 1 BvR 209, 269, 362, 420, 440, 484/83,

www.privacyinternational.org/reports/germany/i-legal-framework (09/02/2012)

Σύμφωνα με το άρθρο 13 (2), το απαραβίαστο του σπιτιού μπορεί να αρθεί μόνο με ένταλμα έρευνας και μπορούν να χρησιμοποιηθούν τεχνικά μέσα για την παρακολούθηση του για να αποτρέψουν κινδύνους για τη δημόσια ασφάλεια. Το άρθρο 13 (3) επιτρέπει την χρήση των τεχνικών μέτρων για την επιτήρηση υπόπτων όπου συγκεκριμένα γεγονότα μπορούν να αποδείξουν ότι ένας ύποπτος έχει διαπράξει σοβαρό έγκλημα. Η χρήση των τεχνικών μέτρων είναι, ωστόσο, περιορισμένη έτσι ώστε να επιτρέπεται μόνο με δικαστική απόφαση. Το άρθρο 13 (4) και (5) επιτρέπει ακουστική παρακολούθηση με σκοπό την πρόληψη από άμεσο κίνδυνο. Το άρθρο 13 άνετο από το άρθρο 17α (2), το οποίο αναφέρει ότι το απαραβίαστο της κατοικίας μπορεί να ανακληθεί από το νόμο, προκειμένου να υπερασπιστεί τη χώρα.

3.2.2 Ο Ομοσπονδιακός νόμος περί προστασίας προσωπικών δεδομένων (Bundesdatenschutzgesetz ή BDSG)

Το 1977 ψηφίστηκε από την Ομοσπονδιακή Δημοκρατία της Γερμανίας ο νόμος (Bundesdatenschutzgesetz ή BDSG)¹⁰³ περί προστασίας εναντίον της καταχρήσεως των προσωπικών δεδομένων κατά την επεξεργασία αυτών, που ισχύει από την 1^η Ιανουαρίου 1978. Ο νόμος τροποποιήθηκε το 1990, το 1994, το 1997, το 2001, όπου ενσωμάτωσε στο γερμανικό δίκαιο τις διατάξεις της κοινοτικής Οδηγίας 95/46/EΚ, το 2006 και τελευταία το 2009. Ο γενικός σκοπός του παρόντος νόμου είναι η προστασία της ιδιωτικής ζωής του ατόμου από την επεξεργασία των προσωπικών του δεδομένων.

Ο νόμος απαγορεύει τη συλλογή, την επεξεργασία και την χρήση των προσωπικών δεδομένων, εκτός εάν υπάρχει η συγκατάθεση¹⁰⁴ του ατόμου που αφορούν οι πληροφορίες, ή η επεξεργασία κρίνεται αναγκαία στη συγκεκριμένη περίπτωση με

¹⁰³ Ομοσπονδιακός νόμος περί προστασίας δεδομένων (BDSG)

¹⁰⁴ Παράγραφος 4 (α) του Ομοσπονδιακού νόμου Bundesdatenschutzgesetz

βάση τις διατάξεις του νόμου ή άλλης ειδικής διαδικασίας. Τα δεδομένα προσωπικού χαρακτήρα πρέπει να συλλέγονται από το υποκείμενο των δεδομένων, η συναίνεση του ατόμου πρέπει να είναι σε γραπτή μορφή και να καθορίζει το πώς, πού, πόσο καιρό, και για ποιο σκοπό τα δεδομένα μπορούν να χρησιμοποιηθούν. Ο υπεύθυνος της επεξεργασίας θα πρέπει να ενημερώνει το υποκείμενο των δεδομένων ως προς την ταυτότητα του, τους σκοπούς της συλλογής, της επεξεργασίας ή της χρήσης, και τις κατηγορίες των αποδεκτών των δεδομένων. Ο πολίτης συχνά βρίσκεται σε σχέση εξάρτησης με οικονομικούς φορείς ή εργοδότες, και είναι εξαναγκασμένος να δώσει τη συγκατάθεση του χωρίς να αποδίδεται η αληθινή του βούληση. Ο εξαναγκασμός ή η δόλια εξαπάτηση για τη χορήγηση συναίνεσης προστατεύονται από τον ΑΚ (παρ.242 BGB) και είναι δυνατή η επίκληση γενικών αρχών ή άλλων προστατευτικών διατάξεων¹⁰⁵.

Ο νομοθέτης προβλέπει την ελεύθερη επεξεργασία των προσωπικών πληροφοριών στο δημόσιο τομέα εφόσον κρίνεται αναγκαία για τη άσκηση των αρμοδιοτήτων της αρχής που της συγκεντρώνει¹⁰⁶ και εφόσον εξυπηρετούν το σκοπό για τον οποίο έχουν συγκεντρωθεί. Η αποθήκευση, η μεταβολή και η χρήση για άλλους σκοπούς επιτρέπεται όταν προβλέπεται από σχετική διάταξη, όταν συναινεί το υποκείμενο των δεδομένων, όταν κρίνεται αναγκαίο για την προστασία του κοινωνικού συνόλου και για επιστημονικούς σκοπούς. Η διοίκηση οφείλει να σέβεται και να τηρεί την αρχή της αναλογικότητας και τις διατάξεις για την προστασία του πολίτη. Η μη τήρηση των διατάξεων αυτών καταστεί την συλλογή και επεξεργασία παράνομη.

Η μετάδοση των προσωπικών πληροφοριών από μια διοικητική αρχή σε άλλη αλλά και η μετάδοση σε τρίτους επιτρέπεται όταν οι πληροφορίες είναι απολύτως αναγκαίες για την άσκηση των αρμοδιοτήτων της αρχής που της κοινοποιεί ή της αρχής που της παραλαμβάνει, και συντρέχουν οι προϋποθέσεις δημοσίευσης κατά την παρ. 14 του νόμου και οι διατάξεις του νόμου απαγορεύουν τη δημοσίευση πληροφοριών για την ικανοποίηση απλής περιέργειας.

¹⁰⁵ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.138

¹⁰⁶ Παράγραφος 13 (1) του Ομοσπονδιακού νόμου Bundesdatenschutzgesetz

Η επεξεργασία πληροφοριών όπως πολιτικές ή θρησκευτικές πεποιθήσεις, συναισθηματική ή γενετήσια ζωή και κατάσταση υγείας, δεν επιτρέπεται, παρά μόνο αν συντρέχουν συγκεκριμένες προϋποθέσεις¹⁰⁷. Επίσης απαγορεύεται επεξεργασία πληροφοριών που αφορούν τη σύνθεση του πορτρέτου της προσωπικότητας ενός ατόμου, που το καθιστά ένα απλό πληροφοριακό αντικείμενο. Σύμφωνα με της διατάξεις του νόμου όλες οι πληροφορίες θεωρούνται σημαντικές και ευαίσθητες και γι' αυτό δεν υπάρχει περαιτέρω διαβάθμιση των ευαίσθητων δεδομένων.

Το υποκείμενο των δεδομένων έχει το δικαίωμα της ενημέρωσης, της αντίρρησης και της διόρθωσης¹⁰⁸. Σύμφωνα με τη διάταξη της παρ.19 εδ.1, ο ενδιαφερόμενος μετά από υποβολή σχετικής αίτησης, η οποία θα πρέπει να προσδιορίζει τα δεδομένα για τα οποία ζητείται η παροχή πληροφοριών, μπορεί να ενημερωθεί για τα δεδομένα που αφορούν στο πρόσωπο του και τον σκοπό της συλλογής τους. Κάθε φορέας που συλλέγει πληροφορίες υποχρεούται να ενημερώνει το πρόσωπο το οποίο οι πληροφορίες αφορούν. Η υποχρέωση ενημέρωσης δεν συντρέχει όταν το υποκείμενο έχει ήδη λάβει γνώση με άλλο τρόπο. Το δικαίωμα της ενημέρωσης συμβάλει στην άσκηση των δικαιωμάτων της συμμετοχής και του ελέγχου και ενισχύει το δικαίωμα της προστασίας και αποτελεί σημαντικό ελεγκτικό μηχανισμό¹⁰⁹. Όταν τα προσωπικά δεδομένα είναι λανθασμένα θα πρέπει να διορθώνονται και να κλειδώνονται¹¹⁰, εφόσον αμφισβητείται η ορθότητα τους από τον ενδιαφερόμενο, θα πρέπει επίσης να διαγράφονται εφόσον η αποθήκευσή τους δεν είναι επιτρεπτή ή όταν η γνώση τους δεν είναι αναγκαία για την άσκηση των καθηκόντων της αρχής.

Ο νομοθέτης διαπιστώνοντας ότι η αυτοματοποιημένη επεξεργασία δεδομένων περιορίζει της ατομικές ελευθερίες, θεσπίζει στον δημόσιο τομέα τον Επίτροπο για την προστασία των δεδομένων¹¹¹ και για τον ιδιωτικό τομέα προβλέπει το διορισμό

¹⁰⁷ Παράγραφος 20 και 35 του Ομοσπονδιακού νόμου Bundesdatenschutzgesetz

¹⁰⁸ Παράγραφος 19 του Ομοσπονδιακού νόμου Bundesdatenschutzgesetz

¹⁰⁹ Α. Γέροντας, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία των προσωπικών δεδομένων, 2002, σελ.145

¹¹⁰ Παράγραφος 35 του Ομοσπονδιακού νόμου Bundesdatenschutzgesetz

¹¹¹ Παράγραφος 22 του Ομοσπονδιακού νόμου Bundesdatenschutzgesetz ,

Επιτρόπου για κάθε αρχείο εφόσον απασχολεί πάνω από 5 εργαζομένους. Μετά από πρόταση της ομοσπονδιακής κυβέρνησης, το γερμανικό Κοινοβούλιο εκλέγει τον Ομοσπονδιακό Επίτροπος για την Προστασία των Δεδομένων και την Ελευθερία των Πληροφοριών¹¹², ο οποίος έχει θητεία 5 ετών και μπορεί να ανανεωθεί άλλη μια φορά. Ο Επίτροπος έχει την υλικοτεχνική υποστήριξη ώστε να τελεί τα καθήκοντα του, υπάγεται στον Υπουργό Εσωτερικών αλλά τελεί ανεξαρτησίας από την Ομοσπονδιακή Κυβέρνηση. Το καθήκον του Επιτρόπου είναι ο έλεγχος των δημοσίων αρχών της Γερμανίας με σκοπό τη συμμόρφωση τους σύμφωνα με το νόμο περί προστασίας προσωπικών δεδομένων και άλλες διατάξεις. Στον έλεγχο του υπόκεινται δεδομένα που συλλέγονται από δημόσιους φορείς μέσω αλληλογραφίας ή τηλεπικοινωνιακών μέσων. Μετά από κάθε έρευνα του ο Επίτροπος είναι υποχρεωμένος να ενημερώνει το δημόσιο φορέα για τα αποτελέσματα της έρευνας καθώς και για τρόπους βελτίωσης. Υποχρεούται επίσης, κάθε δυο χρόνια να υποβάλει αναφορά στην Ομοσπονδιακή βουλή, με την οποία θα ενημερώνει τόσο τη Βουλή, όσο και το κοινό για της εξελίξεις στο θέμα της προστασίας των δεδομένων.

Ο Ομοσπονδιακός νόμος αναφέρεται σε μεμονωμένα στοιχεία που αφορούν την προσωπική ή αντικειμενική κατάσταση συγκεκριμένου προσώπου, ή προσώπου που μπορεί να προσδιορισθεί και δεν περιλαμβάνει πληροφορίες για επιχειρήσεις, ενώσεις ατόμων ή σωματεία. Προστατεύει της προσωπικές πληροφορίες κατά τη διάρκεια της επεξεργασίας από υπολογιστές, δηλαδή από αυτοματοποιημένη επεξεργασία ενώ οι παραδοσιακές μορφές συλλογής, δηλαδή η μη αυτοματοποιημένη επεξεργασία δεν υπάγεται στον νόμο αυτό. Άλλη μια εξαίρεση του νόμου είναι η επεξεργασία των πληροφοριών από επιχειρήσεις του τύπου, της ραδιοφωνίας και του κινηματογράφου, εφόσον η επεξεργασία των πληροφοριών έχει σκοπό τη δημοσιότητα. Αυτό το προνόμιο των μέσων μαζικής ενημέρωσης επιδιώκει την προστασία της ελευθερίας του τύπου και των άλλων μέσων ενημέρωσης, η οποία είναι κατοχυρωμένη από το άρθρο 5 παρ.1 του Γερμανικού Συντάγματος.

Στη Γερμανία αναφέρεται για πρώτη φορά ειδική διάταξη για την προστασία δεδομένων στο ίντερνετ στον Ομοσπονδιακό Νόμο για τα Πολυμέσα (Information- und

¹¹² www.bfdi.bund.de (14/02/2013)

Kommunikationsdienste-Gesetz, IuKDG) της 22^{ης} Ιουλίου 1997. Στο άρθρο 2 παράγραφος 4 του νόμου, επιβάλλεται η υποχρέωση στους παρόχους υπηρεσιών ίντερνετ να προσφέρουν στους χρήστες τη δυνατότητα ανώνυμης πρόσβασης και πληρωμής με τη χρήση ψευδώνυμου όταν αυτό είναι τεχνικά επιτεύξιμο. Ο νόμος απαγορεύει τη δημοσίευση στοιχείων του χρήστη σε τρίτους χωρίς τη συγκατάθεση του, όπως επίσης και τη χρήση τους για σκοπούς εμπορικούς ή δημοσκοπικούς με σκοπό την έρευνα αναγκών και υπηρεσιών. Τα δεδομένα των χρηστών, πέραν αυτών που χρειάζονται για να γίνει η σύνδεση, δεν επιτρέπεται να τηρηθούν σε διάστημα μεγαλύτερο των 80 ημερών, και αυτό μόνο για την τιμολόγηση υπηρεσιών. Στο χρήστη δίνεται το δικαίωμα απευθείας πρόσβασης (on line)¹¹³.

3.3 Γαλλία [ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ]

Η Γαλλία είναι μια από τις πρώτες χώρες που ψήφισε νομοθεσία για την προστασία των προσωπικών δεδομένων. Η αλματώδης ανάπτυξη των ηλεκτρονικών υπολογιστών, τη δεκαετία του 1970, οδήγησαν τον πρωθυπουργό της Γαλλίας να απευθύνει ερώτημα στο conseil d' Etat, το οποίο σύνελθε και γνωμοδότησε παίρνοντας θέση πάνω στο πρόβλημα, παραδέχεται ότι υπάρχει πρόβλημα και είναι επείγον, υπογραμμίζοντας το γεγονός ότι ο αλματώδης πολλαπλασιασμός των ηλεκτρονικών υπολογιστών θα δημιουργήσει ένα νέο πολιτισμό των πολιτισμό της πληροφορίας, στον οποίο η αναζήτηση της πληροφορίας θα είναι αποδεκτή και η κατοχή αυτής πηγή δύναμης. Για την πρόληψη του κινδύνου αυτού το conseil d' Etat έκανε ορισμένες υποδείξεις προς την κυβέρνηση, η οποία συγκρότησε ειδική επιτροπή από κρατικούς λειτουργούς, συντάσσοντας μια αναφορά 500 σελίδων με τίτλο << Informatique et libertes >> για την αντιμετώπιση του προβλήματος. Η κυβέρνηση κατέθεσε νομοσχέδιο

¹¹³ Γ. Γιαννόπουλος, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002,

το οποίο μετά από μακρές συζητήσεις στην Εθνοσυνέλευση και στη Γερουσία έγινε ο Νόμος Νο 78-17 της 6^{ης} Ιανουαρίου 1978 επί της Informatique των αρχείων και των ελευθεριών.¹¹⁴

3.3.1. Ο Νόμος Νο 78-17 της 6^{ης} Ιανουαρίου 1978 επί της Informatique

Ο νόμος ορίζει ότι η Informatique θα πρέπει να είναι στην υπηρεσία των πολιτών, να μην θίγει τα δικαιώματα του ανθρώπου στην ιδιωτική ζωή και τις ατομικές ελευθερίες, να σέβεται την ανθρώπινη υπόσταση και να λειτουργεί στα πλαίσια της διεθνούς συνεργασίας.

Ο νόμος προβλέπει τη δημιουργία της Εθνικής Επιτροπής για την Προστασία των Δεδομένων και τις Ελευθερίες¹¹⁵ C.N.I.L. (Commission Nationale de l'information et des libertés), μιας ανεξάρτητης διοικητικής αρχής η οποία επιβλέπει την συμμόρφωση με το νόμο όλων των εμπλεκόμενων με τη συλλογή, αποθήκευση και επεξεργασία δεδομένων. Η Εθνική Επιτροπή συντελείται από 17 άτομα που απαρτίζουν όλη την πολιτειακή δομή της χώρας και προέρχονται: 2 μέλη από το Κοινοβούλιο, 2 μέλη από τη Γερουσία, 2 μέλη από το οικονομικό και κοινωνικό συμβούλιο, 6 μέλη από τα Γαλλικά δικαστήρια, 3 μέλη με διάταγμα βάση των γνώσεων τους στην πληροφορική και 2 μέλη που διορίζονται από τον πρόεδρο του Κοινοβουλίου και τον πρόεδρο της Γερουσίας.

Η Επιτροπή δέχεται παράπονα και καταγγελίες από πολίτες και παρεμβαίνει στους οργανισμούς και της υπηρεσίες που καταγγέλλθηκαν, παρέχει πληροφορίες

¹¹⁴ Μαρίνος Α., Ηλεκτρονικοί υπολογιστές και το δίκαιο: informatique juridique, 1980, σελ.75-6 με παραπομπές σε α) A. Holleaux, Revue Administrative, No 181, 1978, σελ.31 και β) J. Frayssinet-P. Kayser, Revue du Droit Public, 1979, σελ. 629

¹¹⁵ Νόμος Νο 78-17, παράγραφος 19 και 24

σχετικά με τα προσωπικά δεδομένα στους πολίτες που θέλουν να ενημερωθούν για τα δικαιώματά τους και ενημερώνει της εταιρίες και τους οργανισμούς για το νόμιμο τρόπο συλλογής και επεξεργασίας προσωπικών δεδομένων. Καθήκον της Επιτροπής είναι να ελέγχει αν εναρμονίζεται ο νόμος σε οποιοδήποτε αρχείο επεξεργάζεται δεδομένα, να δημοσιοποιεί τη διαδικασία της έρευνας, καθώς και το είδος της επεξεργασίας, τον λόγο, την τοποθεσία και τις κατηγορίες ατόμων που λαμβάνουν αυτές τις πληροφορίες. Σε περίπτωση που υπάρχει παράβαση του νόμου η Επιτροπή ειδοποιεί τον υπεύθυνο επεξεργασίας ή ακόμη και τον εισαγγελέα σε πιο σοβαρές υποθέσεις. Κάθε έτος η Επιτροπή παρουσιάζει μια αναφορά στον Πρόεδρο της Γαλλίας και στο Κοινοβούλιο με την οποία ενημερώνει για της δραστηριότητες της το έτος που πέρασε, καθώς και μια περίληψη των υποθέσεων που ανέλαβε και τα αποτελέσματα τους¹¹⁶.

Ο νόμος ορίζει ότι καμία δημόσια αρχή δεν μπορεί να χρησιμοποιήσει ηλεκτρονικό αρχείο για την επεξεργασία προσωπικών δεδομένων αν δεν το επιτρέπει ο νόμος ή κανονιστική πράξη, η οποία θα εκδοθεί μετά από αιτιολογημένη γνώμη της Εθνικής Επιτροπής.¹¹⁷ Όσον αφορά τους ιδιώτες, κανένας ιδιώτης δεν μπορεί να διατηρεί ηλεκτρονικό αρχείο επεξεργασίας ονομαστικών πληροφοριών, εάν πρώτα δεν το δηλώσει στην Εθνική Επιτροπή αναλαμβάνοντας την υποχρέωση τήρησης του νόμου.¹¹⁸

Πληροφορίες που αφορούν ευαίσθητα προσωπικά δεδομένα, όπως φυλετική προέλευση και πολιτικές ή θρησκευτικές πεποιθήσεις απαγορεύεται να συγκεντρωθούν, εκτός αν αυτό γίνει με τη συναίνεση του υποκειμένου των δεδομένων ή από πολιτικές, εκκλησιαστικές και συνδικαλιστικές οργανώσεις και αφορούν τα μέλη τους.¹¹⁹

Το υποκείμενο των δεδομένων έχει το δικαίωμα της ενημέρωσης και το δικαίωμα της διαγραφής τους αν είναι λανθασμένες, ανακριβείς και απαγορεύεται να

¹¹⁶ Μαρίνος Α., Ηλεκτρονικοί υπολογιστές και το δίκαιο, δευτ. έκδοση, 1991, σελ.95

¹¹⁷ Νόμος Νο 78-17, παράγραφος 15

¹¹⁸ Νόμος Νο 78-17, παράγραφος 16

¹¹⁹ Μαρίνος Α., Ηλεκτρονικοί υπολογιστές και το δίκαιο, δευτ. έκδοση, 1991, σελ.96

καταχωρηθούν. Αν μια λανθασμένη ή ανακριβείς πληροφορία έχει δημοσιευθεί σε τρίτους πρέπει να κοινοποιηθεί και η διόρθωση της. Σε περίπτωση αμφισβήτησεως το βάρος της αποδείξεως πέφτει σε αυτόν που έκανε την επεξεργασία εκτός εάν το υποκείμενο έχει δώσει την συγκατάθεση του για την πληροφορία αυτή.¹²⁰

Ιδιαίτερης σημασίας είναι η διάταξη του άρθρου 2 με την οποία ορίζεται ότι καμιά δικαστική απόφαση που αναφέρεται σε εκτίμηση ανθρώπινης συμπεριφοράς (καταγραφή βιοπορτρέτου) δεν επιτρέπεται να έχει σαν βάση το αποτέλεσμα ηλεκτρονικής επεξεργασίας προσωπικών δεδομένων, ενώ σε περίπτωση που πρόκειται για διοικητική απόφαση, ο νόμος ορίζει ότι η απόφαση αυτή δεν πρέπει να έχει σαν μοναδικό στήριγμα το αποτέλεσμα μιας τέτοιας επεξεργασίας.¹²¹

Στο άρθρο 41 του νόμου περιέχονται ποινικές διατάξεις οι οποίες προβλέπουν σε ορισμένες περιπτώσεις πρόστιμο 2.000.000 γαλλικών φράγκων και φυλάκιση έως 5 ετών ιδίως σε περιπτώσεις που παραβιάζεται το επαγγελματικό απόρρητο.¹²²

3.3.2 Υποθέσεις χρήσης προσωπικών δεδομένων.

Το 2003, μέσω του διαδικτύου, έγινε προσβάσιμο σε όλους τους ιδιοκτήτες ακινήτων αρχείο που περιείχε δεδομένα σχετικά με τη μη πληρωμή χρέους από μίσθωση ακινήτου. Η Ανεξάρτητη Γαλλική Αρχή C.N.I.L. κλήθηκε να εκδώσει

¹²⁰ Νόμος Νο 78-17, παράγραφος 34

¹²¹ Μαρίνος Α., Ηλεκτρονικοί υπολογιστές και το δίκαιο: informatique juridique, 1980, σελ.79

¹²² www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (10/04/2013)

απόφαση για τα όρια μιας τέτοιας απόφασης.¹²³ Η απόφαση της Αρχής έθεσε τους ακόλουθους όρους για την νομιμότητα αυτής της δημοσίευσης:

- Ο μισθωτής θα πρέπει να ενημερωθεί, πριν από οποιαδήποτε δημοσίευση δεδομένων, ότι αν δεν τηρήσει τις υποχρεώσεις του, θα τεθεί στη μαύρη λίστα με τα δυσμενή οικονομικά δεδομένα και με ειδική ρήτρα στη σχετική σύμβαση μίσθωσης.
- Δικαίωμα χρήσης της ανωτέρας λίστας έχουν μόνο όσοι ασχολούνται επαγγελματικά με συμβάσεις ακινήτων και όχι όλοι οι ιδιοκτήτες ακινήτων, προσβάλλοντας έτσι την Οδηγία 95/46 για την κατηγοριοποίηση των σκοπών της επεξεργασίας.
- Η δημοσίευση κατ' αυτόν τον τρόπο προσωπικών δεδομένων που αφορούν δικαστικές διαδικασίες απαγορεύεται από το άρθρο 30 του νόμου Νο 78-17 της 6^{ης} Ιανουαρίου 1978 και από το άρθρο 226 του Γαλλικού ποινικού κώδικα.¹²⁴

Σε μια υπόθεση επεξεργασίας δεδομένων από τις αστυνομικές και δικαστικές αρχές το 2001 η Γαλλική Ανεξάρτητη Αρχή κλήθηκε να αντιμετωπίσει το θέμα αρχείου του υπουργείου Εσωτερικών, που είχε ως περιεχόμενο δεδομένα που συλλέγουν οι αστυνομικές αρχές για την διερεύνηση σοβαρών εγκλημάτων αλλά και παραβατικής συμπεριφοράς, με σκοπό την εξιχνίαση των εγκλημάτων αλλά και τη χρήση αρχείου για στατιστικούς σκοπούς.¹²⁵ Η Ανεξάρτητη Αρχή έθεσε όρους για τη χρήση του αρχείου αυτού σύμφωνα με τους οποίους:

- Ο περιορισμός της χρήσης του αρχείου αυτού για την εκάστοτε διερευνώμενη υπόθεση και η μη χρήση και άντληση δεδομένων ανά πάσα στιγμή.
- Ο στενός ορισμός των κριτηρίων σύμφωνα με τα οποία θα εντάσσονται κατηγορίες ατόμων στο αρχείο.

¹²³ Νουσκάλης Γ., Ποινική προστασία προσωπικών δεδομένων : η ομολογιακή συμβολή στην ερμηνεία βασικών όρων, β' εκδ., 2007, σελ.28-9

¹²⁴ www.cnil.fr/english/topics/blacklists/accessible/non/ (10/04/2013)

¹²⁵ Νουσκάλης Γ., Ποινική προστασία προσωπικών δεδομένων : η ομολογιακή συμβολή στην ερμηνεία βασικών όρων, β' εκδ., 2007, σελ.130

- Η χορήγηση στο θύμα της αξιόποινης πράξης του δικαιώματος της πρόσβασης στο αρχείο αυτό, μετά από τελεσίδικη καταδίκη του δράστη του εγκλήματος.
- Η απαγόρευση της χρήσης ευαίσθητων προσωπικών δεδομένων από το αρχείο αυτό, εκτός εάν αυτά προκύπτουν από την ίδια τη φύση των τελεσθέντων εγκλημάτων.

Όσον αφορά την παρακολούθηση των ηλεκτρονικών επικοινωνιών των εργαζομένων¹²⁶, η Ανεξάρτητη Αρχή αποφάνθηκε ότι: α) ως προς τη χρήση του διαδικτύου δεν νοείται γενική απαγόρευση πρόσβασης ή καθολική επιτήρηση των ιστοσελίδων που επισκέπτονται οι εργαζόμενοι, αλλά επιτρέπονται εσωτερικοί κανονισμοί που να απαγορεύουν τη χρήση ορισμένων ιστοσελίδων από το προσωπικό, με συγκεκριμένα ηλεκτρονικά μέσα, μετά πάντα από ενημέρωση που τους έχει γίνει. Μετά από γνωμοδότηση της Αρχής επιτρέπεται η δημιουργία αρχείου αποθήκευσης με μέγιστη διάρκεια τήρησης δεδομένων τους 6 μήνες, στο οποίο θα τηρούνται τα δεδομένα επίσκεψης σε ιστοσελίδες των εργαζομένων, με σκοπό την οικονομική οργάνωση της επιχείρησης ανά τερματικό εργαζομένου, και αυτό μόνο με την τήρηση της υποχρέωσης ενημέρωσης του προσωπικού. β) Αναφορικά με τη χρήση ηλεκτρονικών μέσων αλληλογραφίας από τους εργαζομένους, δεν επιτρέπεται η γενική απαγόρευση της χρήσης τους, ωστόσο επιτρέπεται να τεθεί ένα όριο στην έκταση των μηνυμάτων και στον αριθμό αυτών, για λόγους εταιρικών δαπανών, όπως επίσης και η αρχειοθέτηση του αριθμού των μηνυμάτων ανά εργαζόμενο. Οι πληροφορίες που αποκτούνται με την εφαρμογή των πληροφοριακών συστημάτων των επιχειρήσεων θεωρούνται ως προσωπικά δεδομένα. Στο γαλλικό θεσμικό πλαίσιο, ο συνδυασμός των νομοθετικών διατάξεων, της νομολογίας και των τοποθετήσεων της αρμόδιας αρχής C.N.I.L., έχει δημιουργήσει ένα ιδιαίτερο προστατευτικό πλαίσιο για τον εργαζόμενο σε σχέση με τη χρήση του διαδικτύου και της ηλεκτρονικής του αλληλογραφίας κατά την εργασία του.¹²⁷

¹²⁶ www.cnil.fr/english/topics/human-resources/ (10/04/2013)

¹²⁷ Νουσκάλης Γ., Ποινική προστασία προσωπικών δεδομένων : η ομολογιακή συμβολή στην ερμηνεία βασικών όρων, β' εκδ., 2007, σελ.131-2

Η Γαλλική Ανεξάρτητη Αρχή σε σχέση με τη χρήση βιομετρικών συστημάτων παρακολούθησης,¹²⁸ αναφέρει σε έκθεση της το 2001 ότι οδηγούν σε καταχώριση προσωπικών δεδομένων, είτε με τα καθαυτά βιομετρικά δεδομένα των ατόμων που παρακολουθούνται, είτε με τα βιομετρικά πρότυπα που αποθηκεύονται, ώστε να αναγνωρίζεται κάθε φορά το υποκείμενο που κάνει χρήση αυτού. Στις περιπτώσεις αυτές εφαρμόζονται οι βασικές κατά το νόμο αρχές της επεξεργασίας όπως η αρχή του σκοπού και της αναλογικότητας. Οι κίνδυνοι για το υποκείμενο των δεδομένων είναι η χρήση τους για σκοπό άλλο από αυτό που έχουν συλλεχθεί, όπως για παράδειγμα για αστυνομική ή δικαστική χρήση. Η Αρχή τόνισε ότι τα δεδομένα που προκύπτουν από τη χρήση βιομετρικών συστημάτων θα πρέπει να αποθηκεύονται σε φορητές συσκευές αποθήκευσης και θα πρέπει να χρησιμοποιούνται μόνο από το προς αναγνώριση υποκείμενο, και αυτό ως ένα είδος ψηφιακού κλειδιού ώστε να του επιτραπεί η είσοδος ή όχι σε ένα ορισμένο χώρο. Η χρήση βιομετρικών συστημάτων που θα αποθηκεύουν δεδομένα σε μια βάση θα επιτρέπεται μόνο και εφόσον επιτάσσεται κάτι τέτοιο από συγκεκριμένη ανάγκη ασφαλείας που δεν μπορεί να ικανοποιηθεί διαφορετικά.¹²⁹

3.4 Ηνωμένο Βασίλειο [ΛΙΑΕΣ]

Στο Ηνωμένο Βασίλειο η δημοσίευση στοιχείων στο διαδίκτυο υπόκειται στο νόμο για την προστασία των προσωπικών δεδομένων (Data Protection Act) και το νόμο για την ελευθερία της πληροφόρησης (Freedom of Information Act). Το 1984 ψηφίστηκε ο Data Protection Act, που είχε ως σκοπό την προστασία των προσωπικών δεδομένων από την αυτοματοποιημένη επεξεργασία τόσο στον ιδιωτικό, όσο και στο

¹²⁸ www.cnil.fr/english/topics/regulating-biometrics/ (10/04/2013)

¹²⁹ Νουσκάλης Γ., Ποινική προστασία προσωπικών δεδομένων : η ομολογιακή συμβολή στην ερμηνεία βασικών όρων, β' εκδ., 2007, σελ.132-3

δημόσιο τομέα. Ο νόμος ακολουθούσε τις γενικές αρχές επεξεργασίας προσωπικών δεδομένων και προέβλεπε ως επιβλέπουσα αρχή ένα μονοπρόσωπο όργανο, τον Data Protection Registrar, που είχε ως καθήκον να προωθεί μεθόδους συμμόρφωσης με το νόμο, όπως την έκδοση κωδίκων συμπεριφοράς και οδηγιών. Το 1998 ο Data Protection Act τροποποιήθηκε εφαρμόζοντας την Οδηγία 95/46, με ισχύ από 1/3/2000. Σύμφωνα με αυτό το νόμο ο Data Protection Registrar ονομάστηκε Επίτροπος Πληροφοριών (Information Commissioner), έχοντας την ευθύνη και για το νόμο για την ελευθερία της πληροφόρησης (Freedom of Information Act).¹³⁰

3.4.1 Ο Data Protection Act 1998

Ο Data Protection Act του 1998 τέθηκε σε ισχύ την 1η Μαρτίου 2000, με τις περισσότερες από τις διατάξεις του είναι αποτελεσματικές από τις 24 Οκτωβρίου 2001. Ο σκοπός του νόμου είναι η προστασία των δικαιωμάτων και της ιδιωτικής ζωής των ατόμων, καθώς και η διασφάλιση ότι τα στοιχεία τους δεν υποβάλλονται σε επεξεργασία χωρίς τη γνώση τους, αλλά με τη συγκατάθεσή τους, όπου αυτό είναι δυνατόν. Ο νόμος καλύπτει τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα πρόσωπα που ζουν, και ορίζει μια κατηγορία των ευαίσθητων προσωπικών δεδομένων που υπόκεινται σε αυστηρότερους όρους για την επεξεργασία τους από ό, τι τα απλά προσωπικά δεδομένα.

Η επεξεργασία προσωπικών δεδομένων θα πρέπει να γίνεται σύμφωνα με τις οχτώ αρχές που ο νόμος ορίζει. Η αρχές αυτές είναι:

- Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι νόμιμη και θεμιτή. Ο υπεύθυνος επεξεργασίας θα πρέπει να εξασφαλίσει ότι στο υποκείμενο των δεδομένων έχει γίνει γνωστό ποια από τα στοιχεία του θα

¹³⁰ Γ. Γιαννόπουλος, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002, σελ.81

χρησιμοποιηθούν, για πόσο καιρό και σε ποιους τρίτους θα δημοσιευθούν. Σύμφωνα με την πρώτη αρχή της προστασίας των δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να αιτιολογεί την επεξεργασία των προσωπικών δεδομένων σύμφωνα με μία από τις ακόλουθες προϋποθέσεις:

1. Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία.
 2. Η επεξεργασία είναι αναγκαία για την εκτέλεση μια σύμβασης με το υποκείμενο των δεδομένων, ή για τη λήψη μέτρων τα οποία έχουν σκοπό τη σύναψη της σύμβασης.
 3. Η επεξεργασία είναι απαραίτητη από μια νομική υποχρέωση.
 4. Η επεξεργασία είναι αναγκαία για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων.
 5. Η επεξεργασία είναι αναγκαία για την απονομή της δικαιοσύνης, η άσκηση των καθηκόντων που απορρέουν από την ψήφιση, η άσκηση των καθηκόντων του Στέμματος ή κυβερνητικής υπηρεσίας, ή οποιοσδήποτε άλλες λειτουργίες δημόσιου χαρακτήρα που ασκούνται προς το δημόσιο συμφέρον.
 6. Η επεξεργασία είναι αναγκαία για την επίτευξη των θεμιτών συμφερόντων του υπεύθυνου ή τρίτων, και δεν θίγει τα δικαιώματα, τις ελευθερίες ή νόμιμα συμφέροντα του υποκειμένου των δεδομένων.
- Τα δεδομένα προσωπικού χαρακτήρα πρέπει να λαμβάνονται μόνο για συγκεκριμένο και νόμιμο σκοπό και δεν υφίστανται περαιτέρω επεξεργασία με οποιοδήποτε τρόπο ασυμβίβαστο με το συγκεκριμένο σκοπό.
 - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με το σκοπό για τον οποίο υφίστανται επεξεργασία.
 - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή, και εφόσον χρειάζεται, να ενημερώνονται.
 - Τα δεδομένα προσωπικού χαρακτήρα τα οποία υφίστανται επεξεργασία για οποιονδήποτε σκοπό, δεν πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα από ό, τι είναι απαραίτητο για το σκοπό αυτό.
 - Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία σύμφωνα με τα δικαιώματα των υποκειμένων των δεδομένων, βάσει του νόμου περί προστασίας των δεδομένων.

- Πρέπει να λαμβάνονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που χρειάζονται για την πρόληψη της μη εξουσιοδοτημένης, ή παράνομης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την τυχαία απώλεια, καταστροφή ή ζημιά σε προσωπικά δεδομένα.
- Τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να μεταφέρονται σε χώρα ή έδαφος εκτός του Ευρωπαϊκού Οικονομικού Χώρου, εκτός εάν η χώρα ή επικράτεια διασφαλίζει επαρκές επίπεδο προστασίας για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.¹³¹

Σε περίπτωση που ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί ευαίσθητα προσωπικά δεδομένα, υπάρχουν και άλλες συνθήκες όπως:

- Το υποκείμενο των δεδομένων έχει δώσει ρητά τη συγκατάθεσή του.
- Η επεξεργασία απαιτείται από το νόμο σε σχέση με την απασχόληση.
- Η επεξεργασία είναι αναγκαία για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου.
- Η επεξεργασία είναι αναγκαία για νομικές διαδικασίες, τη λήψη νομικών συμβουλών, ή για την ίδρυση ή την υπεράσπιση των νόμιμων δικαιωμάτων.
- Οι πληροφορίες έχουν δημοσιοποιηθεί από το υποκείμενο των δεδομένων.
- Η επεξεργασία είναι απαραίτητη για την απονομή της δικαιοσύνης, ή για άσκηση των καθηκόντων που απορρέουν από την υιοθέτηση καθηκόντων του Στέμματος ή κυβερνητικής υπηρεσίας.
- Η επεξεργασία είναι απαραίτητη για την απονομή της δικαιοσύνης, η άσκηση των καθηκόντων που απορρέουν από την υιοθέτηση, ή την άσκηση των καθηκόντων του Στέμματος ή κυβερνητικής υπηρεσίας.
- Η επεξεργασία είναι αναγκαία για ιατρικούς σκοπούς, και πραγματοποιείται από έναν επαγγελματία υγείας, ή ένα άτομο με ισοδύναμη υποχρέωση εχεμύθειας.
- Η επεξεργασία είναι αναγκαία για την ανίχνευση της ισότητας των ευκαιριών μεταξύ των ανθρώπων διαφορετικής φυλετικής ή εθνολογικής καταγωγής,

¹³¹ www.soas.ac.uk/infocomp/dpa/policy/overview (08/04/2013)

διαφορετικές θρησκευτικές πεποιθήσεις, ή διαφορετικές καταστάσεις σωματικής ή ψυχικής υγείας, ή σωματικές ή ψυχικές παθήσεις.

- ο Η επεξεργασία είναι το σημαντικό δημόσιο συμφέρον.¹³²

Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται από την καταστροφή, την απώλεια, τη μη εξουσιοδοτημένη πρόσβαση ή κοινοποίηση. Σε περίπτωση που ο υπεύθυνος επεξεργασίας δημοσιοποιεί τα δεδομένα σε έναν “επεξεργαστή δεδομένων”¹³³, αν και θα εξακολουθεί να είναι ο ελεγκτής των δεδομένων που τελικά αποφασίζει τι συμβαίνει στα δεδομένα, θα πρέπει να συνάψει σύμβαση μεταποίησης η οποία πρέπει να γίνεται γραπτώς και πρέπει να ορίζεται το τι ο επεξεργαστής των δεδομένων μπορεί ή δεν μπορεί να κάνει με τα προσωπικά δεδομένα, όπως τα μέτρα ασφαλείας που πρέπει να ληφθούν για την προστασία των δεδομένων. Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να κρατήσουν το δικαίωμα να ελέγχουν τους επεξεργαστές δεδομένων, προκειμένου να διασφαλιστεί η συμμόρφωση με τη σύμβαση.¹³⁴

Το υποκείμενο των δεδομένων έχει το δικαίωμα της πρόσβασης στα προσωπικά του δεδομένα, το δικαίωμα να αντιταχθεί στην επεξεργασία ορισμένων, το δικαίωμα να αντιταχθεί στην αυτοματοποιημένη λήψη αποφάσεων και το δικαίωμα να αντιταχθεί σε άμεσο μάρκετινγκ. Το πιο σημαντικό από αυτά τα δικαιώματα είναι το δικαίωμα της πρόσβασης στα προσωπικά δεδομένα. Ένα άτομο μπορεί να ζητήσει πρόσβαση σε όλα τα προσωπικά δεδομένα των οποίων είναι υποκείμενο, και τα οποία βρίσκονται υπό επεξεργασία από τον υπεύθυνο της επεξεργασίας των δεδομένων. Η αίτηση γίνεται γραπτώς και καταβάλλεται το αντίτιμο μέχρι και £10. Το υποκείμενο υποχρεούται με

¹³² www.soas.ac.uk/infocomp/dpa/policy/overview (08/04/2013)

¹³³ Ένας επεξεργαστής δεδομένων είναι ένα τρίτο πρόσωπο που διορίζεται από τον υπεύθυνο της επεξεργασίας των δεδομένων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για λογαριασμό του.

¹³⁴ www.out-law.com/page-413 (08/04/2013)

την αίτηση του να παρέχει επαρκείς πληροφορίες για τον εντοπισμό και την επαλήθευση της ταυτότητας του.¹³⁵

Ο νόμος ορίζει τον διορισμό Επιτρόπου προστασίας προσωπικών δεδομένων από το Στέμμα, λειτουργώντας όμως ανεξάρτητα. Ο Επίτροπος έχει ως ρόλο να εποπτεύει τη νομοθεσία όσον αφορά τα προσωπικά δεδομένα, να διασφαλίζει ότι οι πολίτες έχουν πρόσβαση στις προσωπικές τους πληροφορίες, και να διασφαλίζει ότι αυτές είναι προστατευμένες. Καθήκοντα του Επιτρόπου είναι η παροχή πληροφοριών προς το κοινό, η δημοσίευση οδηγιών και πληροφοριών για τη σωστή χρήση και διάθεση των προσωπικών δεδομένων, επίλυση παραπόνων πολιτών, διατήρηση αρχείου των υπευθύνων επεξεργασίας δεδομένων, και ανάληψη πρωτοβουλιών ώστε να βελτιωθεί η προστασία των προσωπικών δεδομένων¹³⁶.

3.4.2 O Freedom of Information Act 2000

Ο Freedom of Information Act 2000 (FOIA) ψηφίστηκε στις 30 Νοεμβρίου 2000 και τέθηκε πλήρως σε ισχύ, σε ολόκληρο τον δημόσιο τομέα, από την 1η Ιανουαρίου 2005. Ο νόμος έχει ως στόχο να καταστήσει την κυβέρνηση πιο ανοικτή και πιο φερέγγυα και δίνει στο κοινό ένα νόμιμο δικαίωμα πρόσβασης στις πληροφορίες που κατέχουν οι δημόσιες αρχές. Ισχύει για πάνω από 100.000 δημοσίων αρχών, συμπεριλαμβανομένων των κεντρικών κυβερνητικών υπηρεσιών, των τοπικών αρχών, σχολείων, υπηρεσιών υγείας, αστυνομίας και μια σειρά από άλλους δημόσιους φορείς.¹³⁷ Ο νόμος δημιουργεί νέα δικαιώματα πρόσβασης του κοινού σε όλους τους

¹³⁵ www.out-law.com/page-413 (08/04/2013)

¹³⁶ www.ico.org.uk/what_we_cover (08/04/2013)

¹³⁷ www.gov.uk/make-a-freedom-of-information-request/organisations-you-can-request-information-from (10/04/2013)

τύπους των πληροφοριών που κατέχονται από τις δημόσιες αρχές, καθορίζει τις εξαιρέσεις από το γενικό δικαίωμα, και τοποθετεί μια σειρά από υποχρεώσεις σχετικά με τις δημόσιες αρχές. Ο σκοπός του νόμου είναι να προωθήσει την αύξηση της διαφάνειας και της λογοδοσίας σε ολόκληρο τον δημόσιο τομέα.

Ο Freedom of Information Act 2000 κάνει μια σειρά από τροποποιήσεις¹³⁸ στο Νόμο περί Προστασίας Δεδομένων του 1998. Ένα από τα πιο σημαντικά είναι ότι ο ορισμός των «δεδομένων»¹³⁹ επεκτείνεται, σε ό, τι αφορά τις δημόσιες αρχές, για να καλύψει όλες τις προσωπικές πληροφορίες που κατέχουν. Αυτό περιλαμβάνει «δομημένα» και «αδόμητα» αρχεία. Ωστόσο, μόνο το δικαίωμα πρόσβασης του υποκειμένου, το δικαίωμα στη διόρθωση και περιορισμένα δικαιώματα αποζημίωσης θα ισχύουν για τη νέα κατηγορία των μη δομημένων δεδομένων. Ο Freedom of Information Act 2000, παρατείνει έτσι τα δικαιώματα πρόσβασης που ήδη υπάρχουν στο πλαίσιο του Data Protection Act του 1998. Η αίτηση από ιδιώτη για πληροφορίες σχετικά με τον εαυτό του, θα εξαιρείται από το Freedom of Information Act και θα συνεχίσει να αντιμετωπίζεται ως αίτηση πρόσβασης του υποκειμένου στο πλαίσιο του νόμου περί προστασίας των δεδομένων. Σε ορισμένες περιπτώσεις, ένα τέτοιο αίτημα μπορεί να περιλαμβάνει την απελευθέρωση των σχετικών πληροφοριών τρίτων. Σε περίπτωση που ο αιτών ζητεί συγκεκριμένα πληροφορίες σχετικά με ένα τρίτο μέρος, ή όταν ένα αίτημα θα περιλαμβάνει την αποκάλυψη προσωπικών πληροφοριών σχετικά με ένα τρίτο πρόσωπο, η αίτηση εμπίπτει στην αρμοδιότητα του Data Protection Act.¹⁴⁰ Ωστόσο, η δημόσια αρχή πρέπει να εφαρμόσει τις αρχές προστασίας των δεδομένων κατά την εξέταση της δημοσιοποίησης των πληροφοριών, σχετικά με τα άτομα που ζουν. Μία δημόσια αρχή δεν μπορεί να αποκαλύψει πληροφορίες τρίτων, εάν κάτι τέτοιο σημαίνει παραβίαση αυτών των αρχών.

Ο νόμος επιβάλλεται από τον Επίτροπο Πληροφοριών¹⁴¹ (ICO), ο οποίος συνδυάζει την εποπτεία τόσο της ελευθερίας της πληροφόρησης και της νομοθεσίας

¹³⁸ www.legislation.gov.uk/ukpga/2000/36/part/VII (10/04/2013)

¹³⁹ www.legislation.gov.uk/ukpga/2000/36/section/68 (10/04/2013)

¹⁴⁰ www.jisclegal.ac.uk/dataprotection/dataprotection.htm (10/04/2013)

¹⁴¹ www.legislation.gov.uk/ukpga/2000/36/section/18 (10/04/2013)

περί προστασίας δεδομένων. Ο νόμος ισχύει μόνο στην Αγγλία, την Ουαλία και τη Βόρεια Ιρλανδία. Υπάρχει ξεχωριστή νομοθεσία για τη Σκωτία που επιβάλλεται από τον Επίτροπο Πληροφοριών της Σκωτίας.¹⁴²

3.5 Καναδάς [ΑΙΛΕΣ]

Στον Καναδά υπάρχουν 2 νόμοι που προστατεύουν τους πολίτες από δημοσίευση προσωπικών τους δεδομένων. Ο Ομοσπονδιακός Νόμος (Privacy Act) του 1983 που αναφέρεται στο δημόσιο τομέα, που υποχρεώνει τα ομοσπονδιακά υπουργεία και τους οργανισμούς να σέβονται τα δικαιώματα της ιδιωτικής ζωής, περιορίζοντας τη συλλογή, τη χρήση και αποκάλυψη των προσωπικών πληροφοριών σε ένα σύνολο δίκαιων κανόνων πληροφοριών, και ο Ομοσπονδιακός νόμος για την προστασία των πληροφοριών και των ηλεκτρονικών εγγράφων (Personal Information Protection and Electronic Documents Act) του 2000 που εφαρμόζεται σε οργανισμούς του ιδιωτικού τομέα από το 2001 με πλήρη εφαρμογή σε όλους τους τομείς από το 2004.¹⁴³

Όσον αφορά το Σύνταγμα οι Καναδοί δεν έχουν εκφράσει συνταγματικό δικαίωμα στην ιδιωτική ζωή, τα δικαστήρια έχουν ερμηνεύσει της παραγράφους 7 και 8¹⁴⁴ του Χάρτη των Δικαιωμάτων και των Ελευθεριών ως προστασία από αδικαιολόγητη εισβολή της ιδιωτικής ζωής. Το τμήμα 7 προβλέπει το δικαίωμα στη ζωή, την ελευθερία και την ασφάλεια του προσώπου και το δικαίωμα να μην εκπέσει των δικαιωμάτων αυτών. Το τμήμα 8 προστατεύει από αδικαιολόγητη έρευνα και

¹⁴² www.legislation.gov.uk/ukpga/2000/36/section/80 (10/04/2013)

¹⁴³ Γ. Γιαννόπουλος, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002, σελ.105

¹⁴⁴ www.laws-lois.justice.gc.ca/eng/const/page-15.html#h-44 (12/04/2013)

κατάσχεση. Η αξία της ιδιωτικής ζωής σε αυτά τα δικαιώματα, ωστόσο, αναγνωρίζεται σε μεγάλο βαθμό στο πλαίσιο της ποινικής νομοθεσίας.¹⁴⁵

3.5.1 Ο Privacy Act του 1983

Ο Privacy Act τέθηκε σε ισχύ, σε συνδυασμό με τον Information Act, την 1η Ιουλίου 1983. Ορίζει (άρθρο 3) ως προσωπικές πληροφορίες όλες τις πληροφορίες που καταγράφονται σχετικά με ένα συγκεκριμένο άτομο, σε οποιαδήποτε μορφή (δηλαδή, βίντεο ή κασέτες ήχου, ή οποιοδήποτε ηλεκτρονικό μέσω ενημέρωσης), συμπεριλαμβανομένων των πληροφοριών σχετικά με την ηλικία, την εκπαίδευση και το ιατρικό ή ποινικό ιστορικό.¹⁴⁶ Ο νόμος ορίζει ότι, όπου είναι δυνατόν, οι πληροφορίες πρέπει να συλλέγονται απευθείας από το άτομο στο οποίο αναφέρονται και το άτομο θα πρέπει να ενημερώνεται για τον σκοπό για τον οποίο συλλέγονται.¹⁴⁷ Προς το συμφέρον της διαφάνειας και της ειλικρίνειας, τα κυβερνητικά όργανα υποχρεούνται να δημοσιεύουν δείκτες που δείχνουν όλες τις προσωπικές πληροφορίες των τραπεζών διατηρούνται από αυτά τα ιδρύματα.

Ο νόμος αναγνωρίζει στους ιδιώτες το νόμιμο δικαίωμα πρόσβασης στα προσωπικά δεδομένα που τους αφορούν από την ομοσπονδιακή κυβέρνηση. Επιβάλλει υποχρεώσεις σχετικά με την ομοσπονδιακή κυβέρνηση όσον αφορά τον τρόπο που συλλέγει, διατηρεί, χρησιμοποιεί και αποκαλύπτει προσωπικές πληροφορίες υπό τον έλεγχό της και βάζει στη θέση ενός ανεξάρτητου διαμεσολαβητή, τον Επίτροπο

¹⁴⁵ www.parl.gc.ca/Content/LOP/ResearchPublications/prb0585-e.htm (12/04/2013)

¹⁴⁶ www.laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html (12/04/2013)

¹⁴⁷ www.laws-lois.justice.gc.ca/eng/acts/P-21/page-2.html (12/04/2013)

Προστασίας Προσωπικών Δεδομένων, για την επίλυση προβλημάτων και την επιβολή της συμμόρφωσης με τη νομοθεσία. Ο Privacy Act εφαρμόζεται μόνο για τα ομοσπονδιακά υπουργεία και τους οργανισμούς που αναφέρονται στο παράρτημα του νόμου.

Η κεντρική αρχή του νόμου της ιδιωτικής ζωής είναι ότι οι προσωπικές πληροφορίες που βρίσκονται υπό τον έλεγχο της κυβέρνησης δεν πρέπει να συλλέγονται, χωρίς τη συγκατάθεση του ατόμου και θα πρέπει να χρησιμοποιούνται από την κυβέρνηση για το σκοπό για τον οποίο οι πληροφορίες ελήφθησαν. Ο νόμος, ωστόσο, περιέχει μια λίστα με δεκατρείς εξαιρέσεις,¹⁴⁸ για τις οποίες επιτρέπεται η συλλογή και η γνωστοποίηση χωρίς τη συγκατάθεση του ατόμου. Μερικές από τις εξαιρέσεις είναι για σκοπούς της κυβέρνησης, για αρχειακούς λόγους, για στατιστικούς λόγους εφόσον λάβει γραπτή δέσμευση ότι η αποκάλυψη των πληροφοριών αυτών θα γίνει σε μορφή ώστε να μην μπορεί να αναγνωριστεί το υποκείμενο των δεδομένων, και για σκοπούς εντοπισμού ατόμων προκειμένου να συλληχθεί χρέος προς όφελος του κράτους.¹⁴⁹

Ο καθένας στον Καναδά έχει το δικαίωμα να υποβάλει αίτηση για την πρόσβαση σε προσωπικές πληροφορίες για το άτομό του, που κατέχονται από την ομοσπονδιακή κυβέρνηση. Αν ένα άτομο δεν είναι ικανοποιημένο με την ακρίβεια των πληροφοριών που λαμβάνει, μπορεί να ζητήσει να διορθωθούν. Εάν η αίτηση απορριφθεί, ο αιτών μπορεί να απαιτήσει την σημειογραφία να συνδεθεί με τις πληροφορίες που περιγράφουν τυχόν διορθώσεις που ζήτησε. Η αίτηση γίνεται γραπτώς στο όργανο της κυβέρνησης που έχει τον έλεγχο των πληροφοριών. Ο νόμος προβλέπει μια σειρά απαλλαγών, που μπορεί να χρησιμοποιήσει ένα θεσμικό όργανο της κυβέρνησης, για να αποφύγει την πρόσβαση σε μέρος ή στο σύνολο των προσωπικών πληροφοριών που κατέχει το ίδρυμα.

Ο νόμος προβλέπει τον διορισμό Επιτρόπου οποίος είναι υπεύθυνος για την τήρηση των δυο νόμων. Ο Επίτροπος ερευνά παράπονα των πολιτών σχετικά με θέματα

¹⁴⁸ www.laws-lois.justice.gc.ca/eng/acts/P-21/page-3.html (12/04/2013)

¹⁴⁹ www.laws-lois.justice.gc.ca/eng/acts/P-21/page-3.html (12/04/2013)

προσωπικών δεδομένων, σε δημόσιο και ιδιωτικό τομέα, και δημοσιεύει πληροφορίες σχετικά με τις πρακτικές διαχείρισης προσωπικών δεδομένων. Οι πολίτες έχουν το δικαίωμα να υποβάλουν παράπονα στον Επίτροπο για δημόσιους φορείς βάσει της παραγράφου 29 του Privacy Act, και για τον ιδιωτικό τομέα βάση της παραγράφου 11 του νόμου για την προστασία των πληροφοριών και των ηλεκτρονικών εγγράφων. Η δράση του επιτρόπου είναι συνήθως μεσολαβητική, κάνοντας διαπραγματεύσεις και συμβιβασμούς, έχει όμως τη δυνατότητα να οδηγήσει την επίλυση στο ομοσπονδιακό δικαστήριο, καλώντας μάρτυρες και ενόρκους. Το ομοσπονδιακό δικαστήριο μπορεί να επιβάλει τη συμμόρφωση και διόρθωση παράνομων πρακτικών συλλογής προσωπικών δεδομένων και να αποζημιώσει τον παραπονούμενο.¹⁵⁰

Εκτός από τη διερεύνηση των καταγγελιών σχετικά με τη λειτουργία του νόμου περί προστασίας προσωπικών δεδομένων, ο Επίτροπος Προστασίας Προσωπικών Δεδομένων μπορεί να διεξάγει ελέγχους των ορθών πρακτικών πληροφοριών, των κρατικών θεσμών, και διεξαγωγή ειδικών μελετών που αναφέρονται στον Επίτροπο από τον Υπουργό Δικαιοσύνης.

3.5.2 Ο Νόμος για την Προστασία Προσωπικών Πληροφοριών και ηλεκτρονικών εγγράφων (P.I.P.E.D.A.)

Τον Ιανουάριο του 1998, βιομήχανοι του Καναδά και Υπουργείο Δικαιοσύνης κυκλοφόρησαν ένα έγγραφο συζήτησης για την προστασία των προσωπικών πληροφοριών, κατά το οποίο διαπιστώθηκε ότι η διασφάλιση της εμπιστοσύνης των καταναλωτών ήταν απαραίτητη για την ανάπτυξη της οικονομίας της πληροφορίας. Το έγγραφο παρατήρησε ότι “νομοθεσία που θεσπίζει ένα σύνολο κοινών κανόνων για την

¹⁵⁰ www.laws-lois.justice.gc.ca/eng/acts/P-21/page-15.html (12/04/2013)

προστασία των προσωπικών δεδομένων θα βοηθήσει στην οικοδόμηση της εμπιστοσύνης των καταναλωτών και τη δημιουργία ισότιμων όρων ανταγωνισμού έτσι ώστε η κακή χρήση των προσωπικών πληροφοριών να μην μπορεί να οδηγήσει σε ανταγωνιστικό πλεονέκτημα”. Το αποτέλεσμα αυτής της διαβούλευσης ήταν η ανάπτυξη στον ιδιωτικό τομέα νομοθεσίας για την προστασία προσωπικών πληροφοριών και των ηλεκτρονικών εγγράφων.

Ο νόμος για την Προστασία Προσωπικών Πληροφοριών¹⁵¹ και τα ηλεκτρονικά έγγραφα εισήχθη για πρώτη φορά στη Βουλή των Κοινοτήτων τον Οκτώβριο του 1998 ως Bill C-54.¹⁵² Εισήχθη εκ νέου ως Bill C-6¹⁵³ τον Οκτώβριο του 1999 κατά την έναρξη της νέας κοινοβουλευτικής περιόδου. Η Γερουσία πέρασε το νομοσχέδιο με δύο τροπολογίες που αφορούν σε προσωπικές πληροφορίες υγείας. Το Κοινοβούλιο ενέκρινε τις τροποποιήσεις και ο νόμος επικυρώθηκε στις 13 του Απρίλη του 2000. Ο νόμος θεσπίζει κανόνες για τη διαχείριση των προσωπικών πληροφοριών από τις οργανώσεις που συμμετέχουν σε εμπορικές δραστηριότητες και επιτυγχάνει μια ισορροπία ανάμεσα στο δικαίωμα του ατόμου στην προστασία των προσωπικών δεδομένων και την ανάγκη των οργανισμών να αποκτήσουν και να χειρίζονται αυτές τις πληροφορίες για νόμιμους επιχειρηματικούς σκοπούς.

Ο P.I.P.E.D.A. θεσπίζει τις 10 αρχές της ιδιωτικής ζωής στο πλαίσιο του καναδικού κώδικα Model Standards Association¹⁵⁴ για την προστασία προσωπικών δεδομένων. Οι αρχές¹⁵⁵ αυτές είναι:

- Υπευθυνότητα: Ο κάθε οργανισμός που έχει στον έλεγχο του πληροφορίες είναι υπεύθυνος για αυτές και θα πρέπει να ορίζει υπεύθυνο επεξεργασίας που θα είναι υπόλογος για τη συμμόρφωση του οργανισμού με τις αρχές αυτές.

¹⁵¹ www.priv.gc.ca/leg_c/legislation/02_06_07_e.asp (12/04/2013)

¹⁵² www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00218.html (12/04/2013)

¹⁵³ www.parl.gc.ca/HousePublication.aspx?Pub=Bill&Doc=c-6_4%Language=&Mode=1&Parl=36&Ses=2&File=16 (12/04/2013)

¹⁵⁴ www.csa.ca/cm/ca/en/privacy-code (12/04/2013)

¹⁵⁵ www.privacysense.net/10-privacy-principles-of-pipeda/ (12/04/2013)

- Προσδιορισμός του σκοπού: Ο προσδιορισμός του σκοπού για τον οποίο συλλέγονται οι πληροφορίες θα πρέπει να προσδιορίζεται πριν ή κατά τη διάρκεια της συλλογής.
- Συγκατάθεση: Το υποκείμενο των δεδομένων θα πρέπει να έχει λάβει γνώση και να έχει δώσει τη συγκατάθεση του για τη συλλογή και επεξεργασία των προσωπικών του δεδομένων, εκτός από περιπτώσεις που προβλέπονται από το νόμο.
- Περιορισμός Συλλογής: Η συλλογή προσωπικών δεδομένων θα πρέπει να περιορίζεται στα δεδομένα τα οποία εξυπηρετούν τον σκοπό για τον οποίο γίνεται η συλλογή.
- Περιορισμός χρήσης, αποκάλυψης και διατήρησης: Τα προσωπικά δεδομένα δεν θα πρέπει να χρησιμοποιούνται, να διατηρούνται ή να δημοσιεύονται για διαφορετικούς σκοπούς από αυτούς για τους οποίους έχουν συλλεγεί, εκτός εάν έχει δώσει την συγκατάθεση του το υποκείμενο των δεδομένων, ή επιβάλλεται από το νόμο.
- Ακρίβεια: Τα προσωπικά δεδομένα θα πρέπει να είναι ακριβής, πλήρης και επίκαιρα ώστε να εξυπηρετούν τους σκοπούς για τους οποίους θα χρησιμοποιηθούν.
- Εγγυήσεις Ασφάλειας: Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με εγγυήσεις ασφάλειας ανάλογες με το πόσο ευαίσθητα είναι.
- Φανερές διαδικασίες: Οι οργανισμοί θα πρέπει να έχουν συγκεκριμένες πληροφορίες που αφορούν την πολιτική και τις πρακτικές που ακολουθούν για την διαχείριση των προσωπικών δεδομένων, έτοιμες ανά πάσα στιγμή.
- Ατομική Πρόσβαση: Κάθε άτομο θα πρέπει να έχει πρόσβαση και να ενημερώνεται μετά από αίτηση του σχετικά με την ύπαρξη, χρήση και επεξεργασία προσωπικών του δεδομένων. Επίσης έχει το δικαίωμα της αμφισβήτησης και της διόρθωσης πληροφοριών που τον αφορούν.
- Αμφισβήτηση Συμμόρφωσης: Κάθε άτομο θα πρέπει να έχει το δικαίωμα να αμφισβητεί τη συμμόρφωση ενός οργανισμού, με τις παραπάνω αρχές, στον αρμόδιο υπεύθυνο επεξεργασίας δεδομένων.

Εξαιρέση από της αρχές αυτές αποτελούν οι πληροφορίες που συλλέγονται, επεξεργάζονται και χρησιμοποιούνται για δημοσιογραφικούς ή καλλιτεχνικούς

σκοπούς, οι πληροφορίες που μπορεί να αλλοιωθούν από την εξασφάλιση της συγκατάθεσης, όταν οι πληροφορίες συμβάλουν σε μια δικαστική κατάσταση, όταν βοηθούν ώστε να σωθεί η ζωή ατόμων που κινδυνεύουν και για την διατήρηση σημαντικών ιστορικών αρχείων

Σύμφωνα με το νόμο οι Καναδοί έχουν το δικαίωμα να γνωρίζουν γιατί μια επιχείρηση ή ένας οργανισμός συλλέγει, χρησιμοποιεί, ή αποκαλύπτει προσωπικές πληροφορίες τους, όπως το όνομα, την ηλικία, ιατρικά αρχεία, έσοδα, δαπάνες και συνήθειες. Δίνει επίσης το δικαίωμα να ελέγχουν τα προσωπικά τους στοιχεία και να διορθώνουν τυχόν ανακρίβειες. Οι επιχειρήσεις πρέπει να λάβουν τη συγκατάθεση του ατόμου όταν συλλέγουν, χρησιμοποιούν ή αποκαλύπτουν προσωπικές πληροφορίες, εκτός από ορισμένες περιπτώσεις, όπως πληροφορίες που είναι απαραίτητες για τη διεξαγωγή έρευνας ή έκτακτης ανάγκης όπου η ζωή ή ασφάλεια βρίσκονται σε κίνδυνο.

Ο νόμος ισχύει για τη συλλογή, χρήση και αποκάλυψη των προσωπικών πληροφοριών από τις οργανώσεις κατά τη διάρκεια της εμπορικής δραστηριότητας.¹⁵⁶ Τα προσωπικά στοιχεία είναι οποιαδήποτε πληροφορία καταγράφεται σχετικά με ένα συγκεκριμένο άτομο και περιλαμβάνουν οργανισμούς, ενώσεις, συνεταιρισμούς, τα πρόσωπα και τα συνδικάτα και δεν ισχύουν για την Ομοσπονδιακή κυβέρνηση που υπόκεινται στο Νόμο Προστασίας Προσωπικών Δεδομένων,¹⁵⁷ για προσωπικές πληροφορίες που συλλέγονται, χρησιμοποιούνται ή γνωστοποιούνται για προσωπικούς λόγους, για προσωπικές πληροφορίες που συλλέγονται και γνωστοποιούνται για δημοσιογραφικούς ή καλλιτεχνικούς σκοπούς, και για πληροφορίες όπως το όνομα, ο τίτλος και η διεύθυνση μιας επιχείρησης.

Οι οργανισμοί μπορούν να συλλέγουν προσωπικές πληροφορίες μόνο για το σκοπό για τον οποίο γίνεται η συλλογή¹⁵⁸ και θα πρέπει να εξηγήσουν γιατί χρειάζονται τις πληροφορίες, που θα χρησιμοποιηθούν, αν σκοπεύουν να τις αποκαλύψουν σε τρίτους, και θα πρέπει να λάβουν συγκατάθεση για τη χρήση. Υπάρχουν εξαιρέσεις για

¹⁵⁶ www.priv.gc.ca/information/02_05_d_08_e.asp (12/04/2013)

¹⁵⁷ www.laws-lois.justice.gc.ca/eng/acts/P-8.6/page-2.html (12/04/2013)

¹⁵⁸ www.laws-lois.justice.gc.ca/eng/acts/P-8.6/page-3.html (12/04/2013)

την παροχή συγκατάθεσης, όπως για την επιβολή του νόμου, για επιστημονικές έρευνες και λόγους έκτακτης ανάγκης.

Τα άτομα έχουν το δικαίωμα της πρόσβασης σε πληροφορίες σχετικά με τον εαυτό τους, που κατέχονται από έναν οργανισμό, και μπορούν να ζητήσουν, αν αυτές είναι ανακριβείς ή ελλιπείς, τη διόρθωση τους. Οι εξαιρέσεις περιλαμβάνουν θέματα όπως η εθνική ασφάλεια, το προνόμιο δικηγόρου-πελάτη, και απειλές για την ασφάλεια των άλλων.

Σύμφωνα με το νόμο, τα άτομα μπορούν να υποβάλουν καταγγελία στον Επίτροπο Προστασίας Προσωπικών Δεδομένων για το πώς οι οργανισμοί χειρίζονται τα προσωπικά τους στοιχεία. Ο Επίτροπος λειτουργεί ως διαμεσολαβητής, λαμβάνει, διερευνά, διενεργεί ελέγχους και επιλύει τα παράπονα των πολιτών. Ένα άτομο που δεν είναι ικανοποιημένο με τα αποτελέσματα της έρευνας από τον Επίτροπο Προστασίας Προσωπικών Δεδομένων, μπορεί να υποβάλει αίτηση στο Ομοσπονδιακό Δικαστήριο για ακρόαση. Το Δικαστήριο μπορεί να χορηγήσει αποζημίωση (συμπεριλαμβανομένων των ζημιών για ηθική βλάβη) και να διατάξει έναν οργανισμό να διορθώσει τις πρακτικές του.¹⁵⁹

3.6 Αυστραλία [ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ]

Το ομοσπονδιακό σύνταγμα της Αυστραλίας και τα συντάγματα των έξι πολιτειών της δεν περιέχουν ρητή προστασία της ιδιωτικής ζωής. Ο κύριος νόμος που καλύπτει την προστασία προσωπικών δεδομένων, είναι ο περί ιδιωτικής ζωής Privacy act του 1988 με τις τροποποιήσεις του. Ο Privacy Act 1988 παρέχει ένα σύστημα για την επιβολή της ιδιωτικής ζωής και κατευθυντήριες γραμμές για τη χρήση προσωπικών πληροφοριών, από τον δημόσιο τομέα μέσω των 11 Αρχών Προστασίας Προσωπικών

¹⁵⁹ www.laws-lois.justice.gc.ca/eng/acts/P-8.6/page-7.html (12/04/2013)

Δεδομένων, και των 10 Εθνικών Αρχών Προστασίας Προσωπικών Δεδομένων που αφορούν οργανώσεις του ιδιωτικού τομέα. Οι Αρχές ασχολούνται με τον τρόπο και το σκοπό, τη συλλογή, την αποθήκευση, την ασφάλεια, την πρόσβαση, την τροποποίηση, τη χρήση και την αποκάλυψη προσωπικών πληροφοριών.¹⁶⁰

Εκτός του Privacy Act, στην Αυστραλία νόμοι όπως ο Privacy and Personal Information Act και ο Spam Act μπορούν μερικές φορές να χρησιμοποιηθούν για την προστασία της ιδιωτικής ζωής. Ο Privacy and Personal Information Act 1988¹⁶¹ προβλέπει το πώς οι οργανισμοί του δημόσιου τομέα διαχειρίζονται προσωπικές πληροφορίες, και περιέχει 12 Αρχές Προστασίας Πληροφοριών, οι οποίες περιλαμβάνουν τη συλλογή, την αποθήκευση, την πρόσβαση και την ακρίβεια, τη χρήση και αποκάλυψη των προσωπικών πληροφοριών. Επιπλέον, ο νόμος ορίζει τον ρόλο του Επιτρόπου Προστασίας Προσωπικών Δεδομένων και δημιουργεί ένα σύστημα για την επιβολή της ιδιωτικής ζωής σε σχέση με το πώς τα προσωπικά δεδομένα διαχειρίζονται.¹⁶²

Ο Spam Act του 2003 ψηφίστηκε από το Αυστραλιανό Ομοσπονδιακό Κοινοβούλιο και ασχολείται ειδικά με την λήψη ανεπιθύμητων εμπορικών ηλεκτρονικών μηνυμάτων, γνωστή και ως spam ή «ανεπιθύμητη αλληλογραφία». Ο Spam Act εισήχθη ως απάντηση στους φόβους για τις επιπτώσεις του spam στην αποτελεσματικότητα των ηλεκτρονικών επικοινωνιών. Ο νόμος απαγορεύει την αποστολή των εμπορικών ηλεκτρονικών μηνυμάτων που αποστέλλονται χωρίς τη συγκατάθεση του αποδέκτη μέσω του ηλεκτρονικού ταχυδρομείου, υπηρεσιών σύντομων γραπτών μηνυμάτων (SMS), και υπηρεσιών μηνυμάτων πολυμέσων (MMS) ή instant messaging. Οι διατάξεις βάσει του νόμου Spam ισχύουν για όλα τα εμπορικά ηλεκτρονικά μηνύματα. Η Αυστραλιανή Αρχή Επικοινωνιών και Μέσων (ACMA)¹⁶³ έχει την ευθύνη για την επιβολή του Spam Act όσον αφορά τη συλλογή των αποδεικτικών στοιχείων και παρέχει στήριξη για την προστασία των Αυστραλών από

¹⁶⁰ www.services.whitecase.com/wcu/getdoc.aspx?pid=4&cid=2 (09/04/2013)

¹⁶¹ www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/ (09/04/2013)

¹⁶² www.law.uts.edu.au/comslaw/factsheets/privacy.html (09/04/2013)

¹⁶³ www.acma.gov.au/WEB/HOMEPAGE/PC=HOME (09/04/2013)

ηλεκτρονική απάτη και κλοπή ταυτότητας. Επιπλέον, η ACMA ρυθμίζει θέματα περιεχομένου στο διαδίκτυο, ασχολείται με καταγγελίες περιεχομένου στο διαδίκτυο, και παρέχει πληροφορίες σχετικά με υπηρεσίες κινητής τηλεφωνίας.¹⁶⁴

Ο Telecommunications Act 1997 ορίζει αυστηρούς κανόνες για τους φορείς παροχής υπηρεσιών μεταφοράς, που αφορούν στη χρήση και την αποκάλυψη προσωπικών πληροφοριών καταναλωτών.¹⁶⁵ Ο Επίτροπος Προστασίας Προσωπικών Δεδομένων θα πρέπει να γνωμοδοτεί σχετικά με τους κώδικες της ιδιωτικής ζωής. Ο Επίτροπος Προστασίας Προσωπικών Δεδομένων έχει το ρόλο της παρακολούθησης και της συμμόρφωσης με το μέρος 13, τμήμα 5 του νόμου, όπου οι φορείς και οι πάροχοι υπηρεσιών μεταφοράς υποχρεούνται να τηρούν λογαριασμούς όλων των γνωστοποιήσεων των προσωπικών πληροφοριών, με μερικές μόνο εξαιρέσεις. Ο νόμος απαιτεί επίσης αποκάλυψη δεδομένων σε υπηρεσίες επιβολής του νόμου μόνο σε ειδικές περιπτώσεις.¹⁶⁶

3.6.1 Ο Privacy act 1988

Ο νόμος προστασίας προσωπικών δεδομένων έχει διατάξεις που ισχύουν για φορείς του δημόσιου τομέα και για ιδιωτικούς φορείς σύμφωνα με την τροποποίηση του 2000. Στον ιδιωτικό τομέα ο νόμος ορίζει ως οργανώσεις: άτομα, νομικά πρόσωπα, εταιρίες και ενώσεις προσώπων, για τις οποίες ισχύει ο νόμος με την προϋπόθεση ότι ο

¹⁶⁴ www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf (09/04/2013)

¹⁶⁵ www.austlii.edu.au/itlaw/articles/Waters_Interception.html (09/04/2013)

¹⁶⁶ www.law.uts.edu.au/comslaw/factsheets/privacy.html (09/04/2013)

κύκλος εργασιών του οργανισμού είναι μεγαλύτερος από 3.000.000 δολάρια. Ιδιοκτήτες μικρών επιχειρήσεων και πολιτικά κόμματα δεν υπάγονται στο νόμο.¹⁶⁷

Ως προσωπικά στοιχεία ο νόμος ορίζει πληροφορίες ή γνώμες, συμπεριλαμβανομένων των πληροφοριών που αποτελούν μέρος μιας βάσης δεδομένων, είτε αληθείς, είτε όχι, και είτε καταχωρούνται σε έντυπο υλικό ή όχι, για ένα άτομο του οποίου η ταυτότητα είναι προφανής, ή μπορεί εύλογα να εξακριβωθεί. Ρυθμίζει τη συλλογή, την αποθήκευση, την πρόσβαση, χρήση, την αποκάλυψη και τη μεταφοράς των προσωπικών δεδομένων.¹⁶⁸

Για να είναι νόμιμη μια συλλογή και επεξεργασία προσωπικών δεδομένων από δημόσιο οργανισμό θα πρέπει να ακολουθεί τις παρακάτω 11 αρχές:¹⁶⁹

Ο τρόπος και σκοπός της συλλογής των προσωπικών πληροφοριών: οι προσωπικές πληροφορίες πρέπει να συλλέγονται με νόμιμο και θεμιτό τρόπο και μόνο για ένα νόμιμο σκοπό για τον οποίο γίνεται η συλλογή, και θα πρέπει να είναι σχετικές με τη δραστηριότητα του συλλέκτη.

Συγκέντρωση των προσωπικών πληροφοριών από το ενδιαφερόμενο άτομο: ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει τέτοια μέτρα (εάν υπάρχουν), για να διασφαλίσει ότι, πριν συλλεγούν οι πληροφορίες ή αν αυτό δεν είναι εφικτό, το ταχύτερο δυνατόν, να γνωστοποιήσει στο υποκείμενο το σκοπό για τον οποίο οι πληροφορίες του συλλέγονται, αν η συλλογή των πληροφοριών του επιτρέπεται ή επιβάλλεται από το δίκαιο και κάθε πρόσωπο ή όργανο ή οργανισμό στον οποίο, είναι συνήθης πρακτική του συλλέκτη να αποκαλύπτει προσωπικές πληροφορίες.

Συγκέντρωση των προσωπικών πληροφοριών γενικά: ο εκτελών την επεξεργασία θα πρέπει να λάβει τέτοια μέτρα (εάν υπάρχουν), όπως είναι, υπό τις

¹⁶⁷ www.alrc.gov.au/publications/5.%20The%20Privacy%20Act%3A%20Name,%20Structure%20and%20Objects/overview-privacy-act (09/04/2013)

¹⁶⁸ www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/what-%E2%80%98personal-information%E2%80%99 (09/04/2013)

¹⁶⁹ www.privacy.gov.au/materials/types/infosheets/view/6541 (09/04/2013)

περιστάσεις, λογικό για να διασφαλιστεί ότι, έχοντας υπόψη το σκοπό για τον οποίο οι πληροφορίες συλλέγονται είναι σχετικές με το σκοπό αυτό, είναι ενήμερες και η συλλογή των πληροφοριών δεν εισβάλλει σε παράλογο βαθμό στις προσωπικές υποθέσεις του συγκεκριμένου ατόμου.

Αποθήκευση και την ασφάλεια των προσωπικών δεδομένων: ο εκτελών την επεξεργασία, που έχει την κατοχή ή τον έλεγχο μιας εγγραφής που περιέχει τα προσωπικά στοιχεία πρέπει να εξασφαλίζει ότι το αρχείο προστατεύεται με τέτοιες εγγυήσεις ασφαλείας, όπως είναι λογικές για τις περιστάσεις να λάβει, από την απώλεια, τη μη εξουσιοδοτημένη πρόσβαση, τη χρήση, την τροποποίηση ή την αποκάλυψη.¹⁷⁰

Πληροφορίες σχετικά με τα αρχεία που τηρούνται: ένας εκτελών την επεξεργασία που έχει την κατοχή ή τον έλεγχο των αρχείων που περιέχουν προσωπικές πληροφορίες, με την επιφύλαξη της ρήτρας 2 της παρούσας αρχής, λαμβάνει τα μέτρα που είναι, υπό τις περιστάσεις, λογικό να επιτρέπει σε κάθε άτομο να διαπιστώσει αν ο κάτοχος του αρχείου έχει τον έλεγχο των οποιωνδήποτε αρχείων περιέχουν προσωπικά του δεδομένα, τη φύση των εν λόγω πληροφοριών, τους λόγους που χρησιμοποιούνται, και το τι πρέπει να κάνει για να έχει πρόσβαση στο αρχείο αυτό.

Η πρόσβαση σε αρχεία που περιέχουν προσωπικές πληροφορίες: το υποκείμενο των δεδομένων δικαιούται να έχει πρόσβαση σε ένα αρχείο που περιέχει προσωπικά του δεδομένα, στο βαθμό που ο κάτοχος του αρχείου επιτρέπεται να παράσχει στο άτομο πρόσβαση σε αυτό το αρχείο, σύμφωνα με τις ισχύουσες διατάξεις οποιουδήποτε νόμου της Κοινοπολιτείας για την πρόσβαση των ατόμων στα έγγραφα.

Τροποποίηση των εγγραφών που περιέχουν προσωπικές πληροφορίες: ο εκτελών την επεξεργασία πρέπει να λάβει τέτοια μέτρα (εάν υπάρχουν), μέσω των κατάλληλων διορθώσεων, διαγραφών και προσθηκών ώστε οι πληροφορίες που βρίσκονται στο αρχείο να είναι ακριβής, πλήρεις και μη παραπλανητικές.

¹⁷⁰ www.services.whitecase.com/wcu/getdoc.aspx?pid=4&cid=2 (09/04/2013)

Ο Εκτελών την επεξεργασία πρέπει να ελέγξει την ακρίβεια των προσωπικών πληροφοριών πριν από τη χρήση: ο εκτελών την επεξεργασία δεν πρέπει να χρησιμοποιεί αυτές τις πληροφορίες χωρίς να λαμβάνει τέτοια μέτρα (εάν υπάρχουν), όπως είναι, υπό τις περιστάσεις, λογικό να διασφαλιστεί ότι, έχοντας υπόψη το σκοπό για τον οποίο οι πληροφορίες έχουν συλλεγεί, προτείνεται να χρησιμοποιηθούν, οι πληροφορίες να είναι ακριβείς, ενήμερες και ολόκληρες.

Προσωπικές πληροφορίες πρέπει να χρησιμοποιηθούν μόνο για συναφείς σκοπούς: Ο εκτελών την επεξεργασία δεν πρέπει να χρησιμοποιήσει τις πληροφορίες, εκτός από το σκοπό για τον οποίο οι πληροφορίες είναι σημαντικές.

Περιορισμοί στη χρήση των προσωπικών πληροφοριών: ο εκτελών την επεξεργασία, που έχει στην κατοχή του ένα αρχείο που περιέχει προσωπικές πληροφορίες που λαμβάνονται για ένα συγκεκριμένο σκοπό, δεν μπορεί να χρησιμοποιήσει τις πληροφορίες για οποιονδήποτε άλλο σκοπό, εκτός εάν: α) το υποκείμενο των δεδομένων έχει συναινέσει, β) ο εκτελών την επεξεργασία πιστεύει εύλογος ότι η χρήση των πληροφοριών για τον σκοπό αυτόν είναι αναγκαία για την πρόληψη ή τον περιορισμό σοβαρής και επικείμενης απειλής για τη ζωή ή την υγεία του ενδιαφερομένου ή άλλου προσώπου, γ) η χρήση των πληροφοριών για τον σκοπό αυτόν απαιτείται από το νόμο, δ) η χρήση των πληροφοριών για τον σκοπό αυτόν είναι λογικά αναγκαία για την εφαρμογή του ποινικού δικαίου.

Όρια για τη δημοσιοποίηση των προσωπικών πληροφοριών: ο εκτελών την επεξεργασία, που έχει στην κατοχή του αρχείο που περιέχει προσωπικά στοιχεία δεν αποκαλύπτει τις πληροφορίες σε ένα πρόσωπο, φορέα ή οργανισμός, εκτός εάν: α) ο ενδιαφερόμενος είναι εύλογος πιθανό να γνωρίζει, ότι οι πληροφορίες αυτού του είδους συνήθως δημοσιεύονται σε αυτό το πρόσωπο, σώμα ή υπηρεσία, β) ο ενδιαφερόμενος έχει συναινέσει στην δημοσιοποίηση, γ) ο κάτοχος πιστεύει ότι η αποκάλυψη είναι απαραίτητη για την πρόληψη ή τον περιορισμό σοβαρής και επικείμενης απειλής για τη ζωή ή την υγεία του ενδιαφερομένου, δ) η αποκάλυψη αυτή απαιτείται ή επιτρέπεται

από το νόμο και ε) η αποκάλυψη είναι λογικά αναγκαία για την εφαρμογή του ποινικού δικαίου ή του νόμου.¹⁷¹

Σύμφωνα με την αναθεώρηση του 2000 στον ιδιωτικό τομέα για να είναι νόμιμη η συλλογή και επεξεργασία θα πρέπει να ακολουθεί τις παρακατω 10 αρχές:¹⁷²

Συλλογή: Ένας οργανισμός δεν πρέπει να συλλέγει προσωπικές πληροφορίες, εκτός εάν οι πληροφορίες είναι απαραίτητες για μία ή περισσότερες από τις λειτουργίες του. Η συλλογή θα πρέπει να γίνεται με νόμιμο και θεμιτό τρόπο. Ο οργανισμός θα πρέπει να λαμβάνει τα κατάλληλα μέτρα, ώστε το άτομο να γνωρίζει το συντομότερο δυνατόν την ταυτότητα του οργανισμού, τους σκοπούς της συλλογής, το αν ο οργανισμός είναι σε θέση να γνωρίζει τις πληροφορίες και τους οργανισμούς στους οποίους αποκαλύπτει τις πληροφορίες αυτές. Εάν αυτό είναι εφικτό, ένας οργανισμός πρέπει να συλλέγει προσωπικές πληροφορίες για ένα άτομο μόνο από το συγκεκριμένο άτομο. Αν η συλλογή γίνεται από άλλο άτομο, θα πρέπει να λαμβάνει εύλογα μέτρα για να εξασφαλίσει ότι το άτομο έχει ενημερωθεί.

Χρήση και αποκάλυψη: Ένας οργανισμός δεν πρέπει να χρησιμοποιεί ή να αποκαλύπτει προσωπικές πληροφορίες, για ένα άτομο, για ένα σκοπό διαφορετικό από τον πρωταρχικό σκοπό της συλλογής, εκτός εάν ο σκοπός σχετίζεται με τον πρωταρχικό σκοπό της συλλογής, το άτομο θα ανέμενε εύλογα ότι ο οργανισμός θα χρησιμοποιήσει ή θα αποκαλύψει τις πληροφορίες για το δευτερεύοντα σκοπό, ή αν το άτομο έχει συναινέσει στη χρήση ή την αποκάλυψη.

Η ποιότητα των δεδομένων: Ένας οργανισμός πρέπει να λαμβάνει εύλογα μέτρα για να βεβαιωθεί ότι τα προσωπικά στοιχεία που συλλέγει, χρησιμοποιεί ή αποκαλύπτει είναι ακριβή, πλήρη και ενήμερα.

Η ασφάλεια των δεδομένων: Ένας οργανισμός πρέπει να λαμβάνει εύλογα μέτρα για να προστατεύσει τις προσωπικές πληροφορίες που κατέχει από την κακή χρήση, την απώλεια, και από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση ή

¹⁷¹ www.lawhandbook.org.au/handbook/ch21s05s02.php (09/04/2013)

¹⁷² www.privacy.gov.au/materials/types/infosheets/view/6583 (09/04/2013)

αποκάλυψη. Ένας οργανισμός πρέπει να λαμβάνει εύλογα μέτρα για να καταστρέψει προσωπικά στοιχεία, εάν δεν είναι πλέον αναγκαία για οποιοδήποτε σκοπό.

Ειλικρίνεια: Ένας οργανισμός πρέπει να καθορίζει σε ένα έγγραφο σαφώς εκτεφρασμένες πολιτικές σχετικά με τη διαχείριση των προσωπικών πληροφοριών. Ο οργανισμός πρέπει να διαθέτει το έγγραφο σε όποιον το ζητήσει. Κατόπιν αιτήσεως ενός προσώπου, ένας οργανισμός πρέπει να λαμβάνει εύλογα μέτρα, για να γνωστοποιήσει στο πρόσωπο το είδος των προσωπικών πληροφοριών που κατέχει, για ποιους σκοπούς, και πώς συλλέγει, κατέχει, χρησιμοποιεί και αποκαλύπτει τις εν λόγω πληροφορίες.

Πρόσβαση και διόρθωση: Αν ένας οργανισμός κατέχει προσωπικές πληροφορίες για ένα άτομο, πρέπει να παρέχει στο άτομο την πρόσβαση και αν χρειαστεί διόρθωση στις πληροφορίες, κατόπιν αιτήματος του ατόμου, εκτός κατά την περίπτωση που θα έθετε σε σοβαρό και άμεσο κίνδυνο τη ζωή ή την υγεία του κάθε ατόμου, για πληροφορίες υγείας, ή αν η παροχή πρόσβασης θα έχει συνέπειες στην ιδιωτική ζωή άλλων ατόμων, και όταν η αίτηση πρόσβασης είναι επιπόλαια και κακόβουλη.

Ανωνυμία: Όπου αυτό είναι νόμιμο και εφικτό, τα άτομα πρέπει να έχουν τη δυνατότητα να μην ταυτίζονται κατά τις συναλλαγές τους με έναν οργανισμό.

Διασυνοριακές ροές δεδομένων: Ένας οργανισμός στην Αυστραλία ή σε εξωτερικό έδαφος μπορεί να μεταφέρει προσωπικές πληροφορίες για ένα άτομο σε κάποιον που βρίσκεται σε μια ξένη χώρα μόνο εάν: η οργάνωση πιστεύει εύλογα ότι ο αποδέκτης των πληροφοριών υπόκειται σε νόμο, δεσμευτική διάταξη ή σύμβαση, η οποία υπεραμύνεται αποτελεσματικά αρχών για θεμιτό χειρισμό των πληροφοριών, που είναι ουσιαστικά παρόμοια με τις Εθνικές Αρχές Προστασίας Προσωπικών Δεδομένων, συναινεί στη μεταφορά και εάν η διαβίβαση είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του ατόμου και της οργάνωσης.¹⁷³

¹⁷³ www.services.whitecase.com/wcu/getdoc.aspx?pid=4&cid=2 (09/04/2013)

Ευαίσθητες πληροφορίες: Ένας οργανισμός δεν πρέπει να συλλέξει ευαίσθητες πληροφορίες για ένα άτομο, εκτός εάν το άτομο έχει συναινέσει, η συλλογή απαιτείται από το νόμο και η συλλογή είναι αναγκαία για την πρόληψη ή τον περιορισμό σοβαρής και επικείμενης απειλής για τη ζωή ή την υγεία του κάθε ατόμου.

Η συγκατάθεση των υποκειμένων των δεδομένων πριν από τη συλλογή και χρήση των προσωπικών δεδομένων επιβάλλεται, σύμφωνα με το νόμο προστασίας προσωπικών δεδομένων, αλλά δεν απαιτείται εάν η επεξεργασία μπορεί να δικαιολογηθεί για άλλους λόγους. Ωστόσο, η συλλογή προσωπικών δεδομένων που είναι ευαίσθητες πληροφορίες απαιτεί τη συγκατάθεση πάντα, εκτός από ορισμένες εξαιρέσεις. Για παράδειγμα, η εξαίρεση μπορεί να εφαρμόζεται όπου οι πληροφορίες συλλέγονται για την υγεία ή για ορισμένους σκοπούς που η συγκατάθεση των υποκειμένων των δεδομένων δεν είναι εφικτή. Συναίνεση σημαίνει ρητή ή σιωπηρή συναίνεση. Ωστόσο, σύμφωνα με τις γενικές αρχές του νόμου, η συγκατάθεση πρέπει να είναι εθελοντική, ενήμερη, και να δίνεται από ένα άτομο με την ικανότητα να παράσχει συναίνεση. Η συναίνεση μπορεί να δοθεί και σε απευθείας σύνδεση¹⁷⁴.

Χρήση των προσωπικών δεδομένων από τρίτους μπορεί να επιτραπεί ως δευτερεύον σκοπός, ο οποίος σχετίζεται με τον κύριο σκοπό της συλλογής, για τους οποίους αποκάλυψη από τον υπεύθυνο επεξεργασίας για το τρίτο μέρος εύλογα αναμένεται από τα υποκείμενα των δεδομένων. Σε περίπτωση που ένας οργανισμός συλλέγει προσωπικά δεδομένα από κάποιον άλλο, θα πρέπει να λαμβάνει εύλογα μέτρα για να εξασφαλίσει ότι το υποκείμενο των δεδομένων έχει λάβει γνώση ορισμένων θεμάτων.

Ο νόμος προστασίας προσωπικών δεδομένων έχει ως στόχο να είναι τεχνολογικά ουδέτερος και ως εκ τούτου δεν ρυθμίζει τα cookies ή ισοδύναμες συσκευές, αλλά ρυθμίζει τα αποτελέσματα των δραστηριοτήτων αυτών δηλαδή, τη συλλογή, τη χρήση και την αποκάλυψη των προσωπικών πληροφοριών. Τα δεδομένα που συλλέγονται μέσω cookies ή ισοδύναμων εφαρμογών μπορεί να είναι προσωπικές πληροφορίες,

¹⁷⁴ www.alrc.gov.au/publications/19.%20Consent/background (09/04/2013)

όπως ορίζεται στο νόμο Προστασίας Προσωπικών Δεδομένων. Στο βαθμό που ο νόμος προστασίας προσωπικών δεδομένων δεν ισχύει, η χρήση των cookies, ή ισοδύναμων εφαρμογών από έναν οργανισμό πρέπει να είναι σύμφωνες με τις 10 αρχές που θεσπίζονται από το νόμο.¹⁷⁵

Παρά το γεγονός ότι ο νόμος Προστασίας Προσωπικών Δεδομένων δεν παρέχει καθοδήγηση ως προς το τι συνιστά αδικαιολόγητα παρεμβατική συλλογή των δεδομένων προσωπικού χαρακτήρα, ο Επίτροπος Πληροφοριών της Αυστραλίας OAIC έχει εκδώσει κατευθυντήριες γραμμές για τις ομοσπονδιακές κυβερνητικές ιστοσελίδες.¹⁷⁶ Αυτές οι κατευθυντήριες οδηγίες συνιστούν ότι αν μια ιστοσελίδα χρησιμοποιεί cookies, δήλωση απορρήτου ή την πολιτική δικτυακού τόπου θα πρέπει να αναφέρει ότι χρησιμοποιούνται και το σκοπό τους. Η αιτιολογία αυτής της σύστασης είναι ότι πολλοί χρήστες της ιστοσελίδας θεωρούν τα cookies ενοχλητικά. Είναι βέλτιστων πρακτικών για να είναι διαφανείς σχετικά με τη χρήση των cookies σε όρους και προϋποθέσεις και την πολιτική απορρήτου.¹⁷⁷

Υπεύθυνο για τη σωστή εφαρμογή του νόμου είναι το γραφείο του Επιτρόπου Πληροφοριών της Αυστραλίας (OAIC). Οι αρμοδιότητες όμως του Επιτρόπου Πληροφοριών της Αυστραλίας δεν περιορίζονται στις διατάξεις αυτού του νόμου αλλά επιβλέπει και α) το νόμο για τις εγκληματικές πράξεις του 1914, β) το νόμο προγραμμάτων σύγκρισης δεδομένων του 1990, γ) το νόμο εθνικής υγείας του 1953 και δ) το νόμο για της τηλεπικοινωνίες του 1997. Το 2001 ο Επίτροπος Πληροφοριών της Αυστραλίας έχει εκδώσει μια σειρά από κατευθυντήριες γραμμές για την ανάπτυξη κώδικα ιδιωτικότητας από τους οργανισμούς με βάση τα όσα ορίζει ο αναθεωρημένος νόμος. Με αυτή την κίνηση δόθηκε ένας μεγάλος βαθμός ευελιξίας στον τρόπο που οι

¹⁷⁵ www.mondaq.com/australia/x/230850/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Australia (09/04/2013)

¹⁷⁶ www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html (09/04/2013)

¹⁷⁷ www.acma.gov.au/WEB/STANDARD/pc=PC_310521 (09/04/2013)

οργανισμοί τηρούν τις υποχρεώσεις τους, και παράλληλα διασφαλίζει ένα ικανοποιητικό επίπεδο προστασίας όσον αφορά τα προσωπικά δεδομένα.¹⁷⁸

3.7 Ιταλία [ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ]

Το 1981 η Ιταλία ψήφισε την υπ' αριθμό 108 (28 Ιανουαρίου 1981) σύμβαση του Συμβουλίου της Ευρωπαϊκής Ένωσης. Το 1996 ψήφισε το νόμο no 675¹⁷⁹ και μετέφερε την οδηγία 95/46/EK στο ιταλικό δίκαιο. Το 2003 ψηφίστηκε ο νόμος προστασίας προσωπικών δεδομένων, no 196 της Ιταλίας που τέθηκε σε ισχύ την 1η Ιανουαρίου 2004. Συγκεντρώνει όλες τις νομοθεσίες και τους κανονισμούς που αφορούν την προστασία των δεδομένων και αντικαθιστά τον νόμο προστασίας προσωπικών δεδομένων (αριθ. 675/1996),¹⁸⁰ ο οποίος είχε τεθεί σε ισχύ τον Μάιο του 1997. Στο πρώτο μέρος του καθορίζει τις γενικές αρχές προστασίας των δεδομένων που ισχύουν για όλους τους οργανισμούς, στο δεύτερο μέρος του, προβλέπει πρόσθετα μέτρα που θα πρέπει να αναλαμβάνονται από οργανώσεις σε ορισμένους τομείς, για παράδειγμα, της υγείας και των τηλεπικοινωνιών, και το τρίτο μέρος αφορά τις κυρώσεις και τα ένδικα μέσα.

¹⁷⁸ www.alrc.gov.au/publications/5.%20The%20Privacy%20Act%3A%20Name,%20Structure%20and%20Subjects/overview-privacy-act (09/04/2013)

¹⁷⁹ www.ics.uci.edu/~kobsa/privacy/Italian-privacy-law.html (14/04/2013)

¹⁸⁰ Γ. Γιαννόπουλος, Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002, σελ.81

3.7.1 Ο νόμος no 196 του 2003

Ο νόμος τέθηκε σε ισχύ την 1^η Ιανουαρίου του 2004 ενσωματώνοντας την οδηγία 2002/58/EK στο ιταλικό δίκαιο. Ισχύει για κάθε προσωπική δραστηριότητα επεξεργασίας δεδομένων που εκτελείται από οποιαδήποτε οντότητα που έχει δημιουργηθεί στο ιταλικό έδαφος και σε άλλες χώρες υπό ιταλική κυριαρχία. Ακόμη όταν μια οικονομική οντότητα εντός Ευρωπαϊκής Ένωσης κάνει χρήση του εξοπλισμού, που βρίσκεται στο ιταλικό έδαφος, είτε αυτοματοποιημένα ή μη αυτοματοποιημένα υπάγεται στο νόμο.¹⁸¹

Η επεξεργασία των προσωπικών δεδομένων από ιδιωτικούς φορείς ή από δημόσιους κερδοσκοπικούς οργανισμούς επιτρέπεται μόνον εφόσον το υποκείμενο των δεδομένων έχει δώσει προηγούμενη συγκατάθεση. Σε ορισμένες περιπτώσεις, (άρθρο 24) η επεξεργασία μπορεί να πραγματοποιηθεί χωρίς την προηγούμενη συγκατάθεση του υποκειμένου των δεδομένων, εφόσον:

- Είναι υποχρέωση που επιβάλλεται από το νόμο ή κανονισμούς της Ευρωπαϊκής Ένωσης,
- Είναι απαραίτητο για την εκπλήρωση των υποχρεώσεων που απορρέουν από μια σύμβαση, της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος, ή για τη συμμόρφωση με συγκεκριμένα αιτήματα που γίνονται από το υποκείμενο των δεδομένων πριν από τη σύναψη της σύμβασης,
- Προέρχονται από δημόσιες λίστες, μητρώα,
- Αφορά έγγραφα ή αρχεία που είναι διαθέσιμα στο κοινό, με την επιφύλαξη των περιορισμών που προβλέπονται από την ισχύουσα νομοθεσία όσον αφορά την κοινοποίηση και τη δημοσιότητα τους,
- Είναι απαραίτητο για τη διασφάλιση της ζωής ή της σωματικής ακεραιότητας ενός τρίτου, για επιστημονικούς ή στατιστικούς σκοπούς.¹⁸²

¹⁸¹ www.garanteprivacy.it/home_en/italian-legislation (14/04/2013)

¹⁸² www.garanteprivacy.it/documents/10160/10704/Data+protection+code (14/04/2013)

Η συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων θα πρέπει, για να είναι νόμιμη, το υποκείμενο των δεδομένων να έχει δώσει γραπτώς τη συγκατάθεση του και να υπάρξει προηγούμενη έγκριση της Αρχής

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει να γίνεται με νόμιμο και θεμιτό τρόπο. Τα δεδομένα θα πρέπει να είναι ακριβή και ενήμερα και να συλλέγονται για προκαθορισμένους, σαφείς και νομίμους σκοπούς. Η διατήρηση των δεδομένων σε μορφή που να επιτρέπουν την αναγνώριση του υποκειμένου δεν θα πρέπει να είναι μεγαλύτερη από αυτή που χρειάζεται για το σκοπό για τον οποίο έχουν συλλεγεί. Σε μια προσπάθεια να απλοποιηθεί η διαδικασία καταγγελιών, ο Επίτροπος έχει δημοσιεύσει ένα έντυπο παραπόνων στην ιστοσελίδα του.

Σύμφωνα με το άρθρο 7¹⁸³ του νόμου, ο χρήστης έχει το δικαίωμα της ενημέρωσης, της διόρθωσης, της ακύρωσης και της μετατροπής σε ανώνυμη μορφή, ή το κλείδωμα των δεδομένων που υφίστανται επεξεργασία παράνομα, συμπεριλαμβανομένων των δεδομένων που δεν χρειάζεται να διατηρούνται για τους σκοπούς για τους οποίους τα έχουν συλλέξει, ή ακολούθως έχουν επεξεργαστεί. Το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται για την προέλευση των προσωπικών δεδομένων, το σκοπό και τη μέθοδο της επεξεργασίας, τα στοιχεία ταυτότητας του υπεύθυνου επεξεργασίας και τα άτομα ή τις κατηγορίες ατόμων που μπορεί να κοινοποιηθούν τα δεδομένα.

Ο χρήστης έχει το δικαίωμα να αντιταχθεί, εν όλο, ή εν μέρει για νόμιμους λόγους, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τον αφορούν, ακόμα και αν είναι συναφή με τους σκοπούς της συλλογής, στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τον αφορούν, εφόσον πραγματοποιείται με σκοπό την αποστολή διαφημιστικού υλικού ή άμεσης πώλησης, ή για τη διεξαγωγή ερευνών αγοράς ή εμπορικής επικοινωνίας. Το υποκείμενο των δεδομένων μπορεί να ασκήσει τα δικαιώματά του με την υποβολή αίτησης στον υπεύθυνο επεξεργασίας, ο οποίος πρέπει να απαντήσει άμεσα. Τυχόν διαφορές, σε περίπτωση που έχουν αποτραπεί από την άσκηση της πρόσβασης, της διαγραφή και της διόρθωσης, μπορούν

¹⁸³ www.privacy.it/privacy-code-en.html (14/04/2013)

να επιλυθούν είτε μέσω των δικαστηρίων ή με την υποβολή καταγγελιών στον Επίτροπο Προστασίας Δεδομένων.¹⁸⁴

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται έτσι ώστε να ελαχιστοποιηθεί, μέσω των κατάλληλων προληπτικών μέτρων ασφαλείας, ο κίνδυνος καταστροφής ή απώλειας, είτε από ατύχημα είτε όχι, η μη εξουσιοδοτημένη πρόσβαση, ή οι λειτουργίες επεξεργασίας που είναι παράνομες ή ασυμβίβαστες με τον σκοπό για τον οποίο τα στοιχεία που έχουν συλλεχθεί. Τα προληπτικά μέτρα ασφαλείας είναι τόσο τεχνικά όσο και οργανωτικά. Ο νόμος προβλέπει μια σειρά ελάχιστων μέτρων ασφαλείας που ισχύουν για την επεξεργασία, είτε με ηλεκτρονικά μέσα είτε όχι. Περιπτώσεις μη τήρησής μπορεί να προκαλέσουν την εφαρμογή ποινικών και διοικητικών κυρώσεων σε κάθε περίπτωση.

Οι υπεύθυνοι επεξεργασίας των δεδομένων πρέπει να λάβουν συναίνεση μετά από ενημέρωση των υποκειμένων των δεδομένων για την αποθήκευση cookies. Ωστόσο, υπάρχει μια απαγόρευση για το δίκτυο ηλεκτρονικών επικοινωνιών να αποκτήσει πρόσβαση σε πληροφορίες αποθηκευμένες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη, και για την αποθήκευση πληροφοριών ή λειτουργιών ελέγχου που εκτελούνται από ένα χρήστη. Ο νόμος έχει θέσει σε εφαρμογή τις διατάξεις που περιέχονται στο E-Communications για την προστασία της ιδιωτικής ζωής της οδηγίας 2002/58/EK,¹⁸⁵ καθώς και της οδηγίας για τη διατήρηση δεδομένων (2006/24/EK)¹⁸⁶. Μία από τις βασικές αρχές είναι ότι για το ηλεκτρονικό μάρκετινγκ απαιτείται από τις οργανώσεις να λάβουν την συγκατάθεση από τους καταναλωτές, πριν από την αποστολή ηλεκτρονικού μάρκετινγκ.¹⁸⁷ Ωστόσο, για σκοπούς απευθείας εμπορικής προώθησης, ο υπεύθυνος επεξεργασίας μπορεί να χρησιμοποιήσει το e-mail του υποκειμένου των δεδομένων, χωρίς τη συγκατάθεσή του, υπό την προϋπόθεση ότι τα στοιχεία αυτά παρέχονται από το υποκείμενο των δεδομένων στο πλαίσιο της πώλησης του ελεγκτή των δεδομένων, ενός προϊόντος ή μιας υπηρεσίας.

¹⁸⁴ www.ipandit.practicallaw.com/9-502-4794 (14/04/2013)

¹⁸⁵ www.eur-lex.europa.eu/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EL:PDF (14/04/2013)

¹⁸⁶ www.eur-lex.europa.eu/LexUriServ.do?uri=CELEX:32006L0024:el:HTML (14/04/2013)

¹⁸⁷ www.itu.int/osg/spu/spam/legislation/legislation_italy_old.html (14/04/2013)

Όσον αφορά τη διατήρηση των δεδομένων, οι πάροχοι επικοινωνιών υπηρεσιών επιτρέπεται να διατηρούν δεδομένα κίνησης μόνο για μια περίοδο έξι μηνών, προκειμένου να αντιμετωπίσουν τις διαφορές σχετικά με την τιμολόγηση των υπηρεσιών που παρέχονται στους συνδρομητές (άρθρο 123 (2)). Μετά την επικύρωση της Σύμβασης του Συμβουλίου εγκλήματος στον κυβερνοχώρο στην Ευρώπη (μέσω του νόμου αριθ. 48/2008, που τροποποίησε το τμήμα 132 του Κώδικα ΑΣ), οι αστυνομικές αρχές έχουν τη δυνατότητα, υπό ορισμένες συνθήκες, να επιβάλουν στον πάροχο υπηρεσιών διαδικτύου και τους φορείς, να διατηρήσουν τα δεδομένα κίνησης στο διαδίκτυο, προκειμένου να πραγματοποιήσουν προδικαστικές έρευνες, με σκοπό την ανίχνευση και καταστολή συγκεκριμένων αδικημάτων. Η διαταγή που εκδίδεται από τις αστυνομικές αρχές πρέπει να κοινοποιείται και να επικυρώνεται από τον αρμόδιο εισαγγελέα.¹⁸⁸

Η διασυνοριακή μεταφορά των δεδομένων εκτός Ιταλίας επιτρέπεται σε όλα τα κράτη μέλη της ΕΕ. Η μεταφορά εκτός της ΕΕ επιτρέπεται εφόσον το υποκείμενο των δεδομένων έχει δώσει ρητά τη συγκατάθεσή του, για τη διαφύλαξη του δημοσίου συμφέροντος ή της ζωής ενός τρίτου, και για υπεράσπιση μιας νομικής αξίωσης. Η μεταφορά σε ένα μη-κράτος της ΕΕ το οποίο εξασφαλίζει επαρκές επίπεδο προστασίας επιτρέπεται από το νόμο.

Ο νόμος ορίζει τη δημιουργία ανεξάρτητης Εθνικής Ρυθμιστικής Αρχής.¹⁸⁹ Η Αρχή είναι υπεύθυνη για την εποπτεία της συμμόρφωσης με τις διατάξεις περί προστασίας της ιδιωτικής ζωής, τη λήψη αναφορών και καταγγελιών από τα υποκείμενα των δεδομένων, καθώς και για να λάβει τα κατάλληλα μέτρα όσον αφορά τις καταγγελίες που υποβάλλονται. Θα πρέπει να διεξάγει έρευνες με στόχο την εξακρίβωση ότι η επεξεργασία είναι σύμφωνη με τους κανονισμούς προστασίας των δεδομένων, να λάβει τα μέτρα ώστε να συμμορφωθούν με τους κανονισμούς τυχόν παραβιάσεις, και να επιβάλλει διοικητικές κυρώσεις σε παράνομες ή αθέμιτες μορφές επεξεργασίας.¹⁹⁰ Η μη συμμόρφωση με τους κανονισμούς προστασίας των δεδομένων

¹⁸⁸ www.ipandit.practicallaw.com/9-502-4794 (14/04/2013)

¹⁸⁹ www.garanteprivacy.it/home_en (14/04/2013)

¹⁹⁰ www.privireal.org/content/dp/italy.php (14/04/2013)

μπορεί να προκαλέσει τόσο ποινικές ή διοικητικές κυρώσεις όπως πρόστιμα, ακόμα και φυλάκιση από 6 μήνες έως 2 χρόνια.¹⁹¹

3.8 Κύπρος [ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ]

Η Κύπρος είναι μια από τις χώρες που θεμελιώνουν στο σύνταγμα τους την προστασία της ιδιωτικής και οικογενειακής ζωής. Στο άρθρο 15 αναφέρει: << Έκαστος έχει το δικαίωμα όπως η ιδιωτική και οικογενειακή αυτού ζωή τυγχάνει σεβασμού. Δεν χωρεί επέμβαση κατά την άσκησης του δικαιώματος τούτου, ειμή τοιαύτη οία θα ήτο σύμφωνος προς τον νόμον και αναγκαία μόνον προς το συμφέρον της ασφαλείας της Δημοκρατίας ή της συνταγματικής τάξεως ή της δημοσίας ασφαλείας ή της δημοσίας τάξεως ή της δημοσίας υγείας ή των δημοσίων ηθών ή της προστασίας των δικαιωμάτων και των ελευθεριών των υπό του Συντάγματος ηγγυημένων εις παν πρόσωπον¹⁹²>>. Τα άρθρο 16 του Συντάγματος αναφέρει το άσυλο της κατοικίας, και το άρθρο 17 αναφέρει ότι όλοι έχουν το δικαίωμα του απορρήτου της αλληλογραφίας, λέγοντας: << Έκαστος έχει το δικαίωμα σεβασμού και διασφάλισεως του απορρήτου της αλληλογραφίας ως και πάσης άλλης επικοινωνίας αυτού, εφ' όσον η τοιαύτη επικοινωνία διεξάγεται διά μέσων μη απαγορευομένων υπό του νόμου>>.

Η Κύπρος ήταν ένα από τα δέκα κράτη που προσχώρησαν στην ΕΕ την 1η Μαΐου 2004. Η συμμόρφωση με την οδηγία 95/46/ΕΚ, αποτελεί σημαντική προϋπόθεση της ένταξης, ήταν εξασφαλισμένη μέσω της εφαρμογής του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα νόμου του 2001. Ο νόμος του 2001 τροποποιήθηκε το 2003, με το νόμο Αρ. 37 (Ι) / 2003, και το 2012 με τον 105(Ι) /2012.¹⁹³ Η τροποποιήσεις αυτές

¹⁹¹ www.garanteprivacy.it/documents/10160/10704/Data+protection+code (14/04/2013)

¹⁹² www.mfa.gov.cy/mfa/mfa2006.nsf/constitution_gr/constitution_gr (11/04/2013)

¹⁹³ [www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B708D98FB15F8D09C2256D9B0032AE61/\\$file/138%28I%29-2001&37%28I%29-2003&105%28I%29-2012_el.pdf?OpenElement](http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B708D98FB15F8D09C2256D9B0032AE61/$file/138%28I%29-2001&37%28I%29-2003&105%28I%29-2012_el.pdf?OpenElement) (11/04/2013)

αφορούν σκοπούς απευθείας εμπορικής προώθησης.¹⁹⁴ Στην Κύπρο το κανονιστικό πλαίσιο συμπληρώνει ο νόμος ο περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών 112(I)/2004 με τις τροποποιήσεις του, νόμος 51(I) του 2012.¹⁹⁵ Ο 112(I)/2004 ρυθμίζει τις ηλεκτρονικές επικοινωνίες και προβλέπει την προστασία των έννομων συμφερόντων των συνδρομητών των δικτύων ηλεκτρονικών επικοινωνιών και υπηρεσιών.

3.8.1 Ο περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα Νόμος 138(I) του 2001 με τις τροποποιήσεις του, 37(I) του 2003 και 105(I) του 2012.

Ο νόμος εφαρμόζεται σε αυτοματοποιημένη και μη αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο. Ο νόμος για την επεξεργασία των προσωπικών δεδομένων πρέπει να πραγματοποιείται από κάτοικο της Κύπρου ή άλλης περιοχής όπου η κυπριακή νομοθεσία εφαρμόζεται, δυνάμει του δημοσίου διεθνούς δικαίου. Ο νόμος εφαρμόζεται ακόμη και όταν ο υπεύθυνος επεξεργασίας, δεν είναι κάτοικος του κράτους, αλλά για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, προσφεύγει σε αυτοματοποιημένα ή άλλα μέσα που υπάρχουν στην Κύπρο. Ο νόμος δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία πραγματοποιείται από φυσικό πρόσωπο για την άσκηση αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων.¹⁹⁶

¹⁹⁴ www.privireal.org/content/dp/cyprus.php (11/04/2013)

¹⁹⁵ [www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/37D957C789729A48C2257A15004BA5A3/\\$file/51%28I%29-2012.pdf?OpenElement](http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/37D957C789729A48C2257A15004BA5A3/$file/51%28I%29-2012.pdf?OpenElement) (11/04/2013)

¹⁹⁶ www.ldlaw.com.cy/services/dataprotection.htm (11/04/2013)

Ο υπεύθυνος της επεξεργασίας θα πρέπει να διασφαλίσει ότι τα δεδομένα υφίστανται νόμιμη και θεμιτή επεξεργασία, συλλέγονται για προκαθορισμένους, σαφείς σκοπούς και δεν χρησιμοποιούνται περαιτέρω για άλλους σκοπούς. Τα δεδομένα θα πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα χρειάζονται για την ικανοποίηση του σκοπού για τον οποίο γίνεται η συλλογή. Αν χρειαστεί, τα δεδομένα θα πρέπει να υποβάλλονται σε ενημέρωση ώστε να είναι ακριβή, και θα πρέπει να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας του υποκειμένου των δεδομένων, μόνο για το χρόνο που χρειάζεται για την πραγματοποίηση των σκοπών της συλλογής.¹⁹⁷ Οι υπεύθυνοι επεξεργασίας δεδομένων μπορούν να συλλέγουν και να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, όταν συναινεί το υποκείμενο των δεδομένων, ή όταν πληρείται μια από τις παρακάτω προϋποθέσεις:

- Ο υπεύθυνος επεξεργασίας δεδομένων επεξεργάζεται τα δεδομένα για να εισέλθει, ή να πραγματοποιήσει μια σύμβαση στην οποία το υποκείμενο των δεδομένων είναι ένα συμβαλλόμενο μέρος.
- Η επεξεργασία ικανοποιεί νομική υποχρέωση του υποκειμένου των δεδομένων ή προστατεύει τα ζωτικά του συμφέροντα.
- Η επεξεργασία είναι αναγκαία για την εκτέλεση του καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή την άσκηση της δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας
- Η επεξεργασία είναι απαραίτητη για την επίτευξη του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας ή ο τρίτος, στον οποίο τα προσωπικά δεδομένα ανακοινώνονται, υπό την προϋπόθεση ότι τα εν λόγω συμφέροντα υπερσχύουν των δικαιωμάτων, των συμφερόντων και των θεμελιωδών ελευθεριών των υποκειμένων των δεδομένων.

¹⁹⁷ www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/responsib_gr/responsib_gr?OpenDocument (11/04/2013)

Η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα επιτρέπεται όταν το υποκείμενο των δεδομένων έχει δώσει τη ρητή συγκατάθεσή του ή όταν μία ή περισσότερες από μια λίστα πιο αυστηρών προϋποθέσεων πληρούνται.¹⁹⁸

Το υποκείμενο των δεδομένων έχει το δικαίωμα της ενημέρωσης (Άρθρο 11), το δικαίωμα της πρόσβασης στις πληροφορίες που τηρούνται σχετικά με το πρόσωπό του (Άρθρο 12), το δικαίωμα της διόρθωσης ή της διαγραφής (Άρθρο 13), και το δικαίωμα της αποζημίωσης (Άρθρο 17).

Ο υπεύθυνος της επεξεργασίας θα πρέπει να ενημερώσει το υποκείμενο για την ταυτότητά του, και τους λόγους για τους οποίους διενεργεί την επεξεργασία. Όπως επίσης και σχετικά με τα πρόσωπα στα οποία θα δοθούν οι πληροφορίες αυτές. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λάβει αντίγραφα των πληροφοριών που κατέχει ο υπεύθυνος επεξεργασίας και τον αφορούν. Μπορεί να ζητήσει από οποιοδήποτε οργανισμό ή φυσικό πρόσωπο να τον ενημερώσει για το ποιες πληροφορίες διατηρεί που τον αφορούν. Για παράδειγμα, μπορεί να υποβάλει αίτημα στην τράπεζα με την οποία συνεργάζεται, σε μία δημόσια υπηρεσία, στον εργοδότη του, σε ασφαλιστική εταιρεία ή σε γιατρό. Το δικαίωμά αυτό ασκείται με την καταβολή του χρηματικού ποσού των 17 Ευρώ¹⁹⁹. Το φυσικό πρόσωπο ή ο οργανισμός που διατηρεί πληροφορίες που τον αφορούν, πρέπει να απαντήσει γραπτώς μέσα σε τέσσερις εβδομάδες. Το εδάφιο (4) του ίδιου άρθρου παρέχει αρμοδιότητα στον Επίτροπο, ύστερα από αίτηση του υπεύθυνου επεξεργασίας, να άρει, εν όλο, ή εν μέρει αυτή την υποχρέωση, όταν η συλλογή και επεξεργασία των δεδομένων γίνεται για σκοπούς άμυνας, εθνικών αναγκών ή αναγκών εθνικής ασφάλειας της Δημοκρατίας ή για την πρόληψη, διακρίβωση, διερεύνηση και δίωξη ποινικών αδικημάτων.²⁰⁰

Αν οι πληροφορίες που τηρούνται από οποιοδήποτε σχετικά με το υποκείμενο είναι λανθασμένες ή ανακριβείς, έχει δικαίωμα να ζητήσει τη διόρθωσή ή διαγραφή

¹⁹⁸ www.egkyklioι.moec.gov.cy/Data/dde2918b.pdf (11/04/2013)

¹⁹⁹ www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/rights_gr/rights_gr?OpenDocument (11/04/2013)

²⁰⁰ www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/EBB3D2DFD991CCC4C22572A60032B214?OpenDocument (11/04/2013)

όλων των πληροφοριών που το αφορούν, αν δεν υπάρχει λόγος διατήρησής τους, ή αν έχουν αποσπαστεί από αυτόν ή άλλο πρόσωπο παράνομα. Η αίτηση γίνεται εγγράφως στον οργανισμό ή το φυσικό πρόσωπο που διατηρεί πληροφορίες που αφορούν το υποκείμενο και πρέπει να εξηγεί ξεκάθαρα και με κατανοητό τρόπο το αίτημά του. Το δικαίωμα αυτό ασκείται με την καταβολή του ποσού των 17 Ευρώ, το οποίο επιστρέφεται αν το αίτημά γίνει αποδεκτό. Το φυσικό πρόσωπο ή ο οργανισμός πρέπει να απαντήσουν στο αίτημά γραπτώς μέσα σε δεκαπέντε ημέρες. Πρέπει να αναφέρουν τις ενέργειες στις οποίες έχουν προβεί ή να εξηγήσουν τους λόγους για τους οποίους δεν έχουν προβεί σε καμία ενέργεια. Αν φυσικό πρόσωπο ή οργανισμός προκάλεσε ζημία λόγω κακού χειρισμού των πληροφοριών, το υποκείμενο έχει το δικαίωμα να διεκδικήσει αποζημίωση από αυτούς.

Σύμφωνα με το άρθρο 15 του νόμου, οι πληροφορίες που αφορούν το υποκείμενο δεν μπορούν να χρησιμοποιούνται για σκοπούς προώθησης προϊόντων ή υπηρεσιών εξ αποστάσεως, εκτός αν έχει δώσει τη γραπτή συγκατάθεσή του.²⁰¹

Ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να μεταφέρει προσωπικά δεδομένα από τον Ευρωπαϊκό Οικονομικό Χώρο μόνον αφού λάβει άδεια για την εν λόγω μεταβίβαση από τον Επίτροπο. Ο Επίτροπος εκδίδει την άδεια μόνον εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα που δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ'εξάιρεση, μετά από άδεια του Επιτρόπου, όταν συναινέσει το υποκείμενο των δεδομένων, όταν η διαβίβαση είναι αναγκαία για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων, ή για την εκτέλεση σύμβασης της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος, όταν η διαβίβαση είναι αναγκαία προκειμένου να διασφαλιστεί ένα ανώτερο δημόσιο συμφέρον και μια σειρά από άλλες εξαιρέσεις.²⁰²

²⁰¹ Στη σελίδα του Επιτρόπου προστασίας προσωπικών δεδομένων υπάρχει το έντυπο υποβολής παραπόνου λήψης ανεπιθύμητων διαφημιστικών μηνυμάτων.
www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/spam_gr/spam_gr?OpenDocument
(11/04/2013)

²⁰² www.egkykloi.moec.gov.cy/Data/dde2918b.pdf (11/04/2013)

Η επεξεργασία των δεδομένων είναι απόρρητη. Θα πρέπει να διεξάγεται αποκλειστικά από πρόσωπα που ενεργούν υπό την εποπτεία του υπευθύνου της επεξεργασίας ή του επεξεργαστή και μόνο μετά από τις οδηγίες τους. Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που εμπλέκονται στην επεξεργασία των δεδομένων. Ο Επίτροπος δίνει κατευθύνσεις σχετικά με τον βαθμό ασφαλείας των δεδομένων και τα μέτρα προστασίας που πρέπει να λαμβάνονται για κάθε κατηγορία δεδομένων, λαμβάνοντας επίσης υπόψη τις τεχνολογικές εξελίξεις.

Ο νόμος διορίζει Επίτροπο για την προστασία των προσωπικών δεδομένων, ο οποίος είναι υπεύθυνος για την παρακολούθηση της εφαρμογής του παρόντος νόμου και άλλες διατάξεις που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, και ο οποίος ασκεί τα καθήκοντα που του έχουν ανατεθεί από αυτό ή οποιοδήποτε άλλο νόμο. Ο διορισμός του Επιτρόπου γίνεται από το Συμβούλιο των Υπουργών σχετικά με την εισήγηση του Υπουργού. Η θητεία του Επιτρόπου είναι για περίοδο τεσσάρων ετών και μπορεί να ανανεωθεί για μία ακόμη θητεία. Οι αρμοδιότητες του Επιτρόπου είναι:²⁰³

- Να εκδίδει οδηγίες για την ομοιόμορφη εφαρμογή των διατάξεων σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.
- Να βοηθά τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν συστήματα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, κατά την εκπόνηση κωδίκων δεοντολογίας, ώστε να προστατευτεί καλύτερα το δικαίωμα στην ιδιωτική ζωή.
- Να υποβάλλει προτάσεις και υποδείξεις στους υπευθύνους ή τους εκπροσώπους τους, και να δώσει, κατά την κρίση του δημοσιότητα σε αυτές.
- Να χορηγεί τις άδειες που προβλέπονται από τον παρόντα νόμο.

²⁰³ www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.CY (11/04/2013)

- Να επιβάλλει διοικητικές κυρώσεις που προβλέπονται από το άρθρο 25 του νόμου.
- Να προβαίνει, με δική του πρωτοβουλία ή κατόπιν καταγγελίας, σε διοικητική έρευνα σε οποιοδήποτε σύστημα αρχειοθέτησης.
- Να λαμβάνει αποφάσεις σχετικά με κάθε ρύθμιση που αφορά την επεξεργασία και προστασία των προσωπικών δεδομένων.
- Να εκδίδει κανόνες, οδηγίες πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, στα οποία αναφέρεται ο παρών νόμος.
- Να συντάσσει ετήσια έκθεση σχετικά με τις δραστηριότητές του κατά το προηγούμενο ημερολογιακό έτος. Η έκθεση αναφέρει επίσης τις απαραίτητες νομοθετικές τροποποιήσεις, που μπορεί να ζητηθούν, στον τομέα της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα
- Να εξετάζει τις καταγγελίες που αφορούν την εφαρμογή του παρόντος νόμου και την προστασία των δικαιωμάτων των αιτούντων, όταν αυτά τίγονται από την επεξεργασία των δεδομένων που τους αφορούν.
- Να τηρεί τα Μητρώα που προβλέπονται από τον παρόντα νόμο.²⁰⁴

3.8.2 Ο Περί Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών Νόμος του 2004, 112(Ι)/2004 με τις τροποποιήσεις του, Νόμος 51(Ι) του 2012.

Ο περί ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών νόμος του 2004 (112 (Ι) / 2004), τροποποιήθηκε με τον νόμο 51(Ι)/2012²⁰⁵ (Νόμος

²⁰⁴ www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/duties_gr/duties_gr?OpenDocument (11/04/2013)

²⁰⁵ www.cylaw.org/nomoi/arith/2012_1_51.pdf (11/04/2013)

Ηλεκτρονικών και Ταχυδρομικών Υπηρεσιών). Ο 51(I)/2012 συμπληρώνει τις διατάξεις του νόμου περί ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και προβλέπει την προστασία των έννομων συμφερόντων των συνδρομητών των δικτύων ηλεκτρονικών επικοινωνιών και υπηρεσιών που είναι νομικά πρόσωπα. Εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα σε σχέση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, στα δίκτυα επικοινωνιών της Κύπρου. Σύμφωνα με το άρθρο 18 του νόμου, ο Επίτροπος Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών έχει την υποχρέωση να προωθήσει τα συμφέροντα των πολιτών της Κύπρου και της Ευρωπαϊκής Ένωσης, μεταξύ άλλων, συμβάλλοντας στην εξασφάλιση υψηλού επιπέδου προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής.

Το άρθρο 98 του νόμου προβλέπει τα κατάλληλα τεχνικά και οργανωτικά μέτρα που πρέπει να λαμβάνονται από παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών και για την διαφύλαξη της ασφάλειας των υπηρεσιών και δικτύων τους.

Το μέρος 14²⁰⁶ του νόμου των Ηλεκτρονικών και Ταχυδρομικών Υπηρεσιών ασχολείται με τη συλλογή των δεδομένων θέσης, των δεδομένων κίνησης και τη χρήση των cookies. Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και τα οποία αποθηκεύουν οι οργανισμοί, θα πρέπει να απαλείφονται ή να καθίστανται ανώνυμα κατά τη λήξη της κλήσης, με εξαίρεση: για την χρέωση των συνδρομητών και εφόσον ο συνδρομητής ή ο χρήστης συναινέσει ότι τα δεδομένα μπορούν να υποβληθούν σε επεξεργασία από μια επιχείρηση, με σκοπό την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών του τελευταίου, ή για την παροχή υπηρεσιών προστιθέμενης αξίας. Η απαγόρευση της αποθήκευσης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών ή χωρίς τη συγκατάθεσή τους δεν αποκλείει την τυχόν αυτόματη, ενδιάμεση και προσωρινή αποθήκευση των πληροφοριών. Στους χρήστες πρέπει να δίνεται η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους για την επεξεργασία των δεδομένων κίνησης.

²⁰⁶ www.cylaw.org/nomoi/enop/non-ind/2004_1_112/index.html (11/04/2013)

Τα δεδομένα θέσης μπορούν να διεκπεραιωθούν μόνο όταν καθίστανται ανώνυμα ή με τη συγκατάθεση των χρηστών στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια, για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Ο φορέας παροχής υπηρεσιών πρέπει να ενημερώνει τους συνδρομητές, προτού δώσουν τη συγκατάθεσή τους για τον τύπο των δεδομένων θέσης που υποβάλλονται σε επεξεργασία, το σκοπό και τη διάρκεια της επεξεργασίας, και αν τα δεδομένα θα διαβιβάζονται σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Στους χρήστες πρέπει να δίνεται η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους για την επεξεργασία των δεδομένων.²⁰⁷

Η φύλαξη και χρησιμοποίηση των cookies και παρόμοιων τεχνολογιών επιτρέπεται μόνο εφόσον ο συνδρομητής έχει σαφείς και αναλυτικές πληροφορίες, μεταξύ άλλων, για τους σκοπούς της επεξεργασίας, και έχει δώσει τη συγκατάθεσή του σύμφωνα με τον περί Επεξεργασίας Προσωπικών Δεδομένων νόμο. Το παραπάνω δεν εμποδίζει οποιαδήποτε τεχνικής φύσεως αποθήκευση ή πρόσβαση, αποκλειστικός σκοπός της οποίας είναι η διενέργεια ή η διευκόλυνση της διαβίβασης μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι αυστηρώς αναγκαία για την παροχή υπηρεσίας που έχει ζητήσει ρητά ο συνδρομητής.²⁰⁸

²⁰⁷ www.mondaq.com/x/230888/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Cyprus (11/04/2013)

²⁰⁸ www.law.com.cy/services/dataprotection.htm (11/04/2013)

ΚΕΦΑΛΑΙΟ 4: ΕΠΙΛΟΓΟΣ-ΣΥΜΠΕΡΑΣΜΑΤΑ

[ΚΑΛΟΓΕΡΟΠΟΥΛΟΣ-ΛΙΛΕΣ]

Η έλευση της τεχνολογίας των πληροφοριών, τη δεκαετία του 1960 και του 1970 αύξησαν το ενδιαφέρον για την προστασία των προσωπικών δεδομένων. Οι δυνατότητες παρακολούθησης, των ισχυρών συστημάτων πληροφορικής απαιτούσαν ειδικούς κανόνες και νομικές ρυθμίσεις που θα προστάτευαν τους πολίτες από την χρήση των δεδομένων τους. Η πρώτη σύγχρονη νομοθεσία στον τομέα αυτό θεσπίστηκε στο κρατίδιο της Έσσης στη Γερμανία το 1970. Στις αρχές του 1970, οι περισσότερες χώρες άρχισαν να θεσπίζουν γενικούς νόμους για την προστασία της ιδιωτικής ζωής του ατόμου και τα προσωπικά δεδομένα. Οι περισσότεροι από αυτούς τους νόμους έχουν ως βάση τα μοντέλα που κυκλοφόρησαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης και από το Συμβούλιο της Ευρώπης.

Σε πολλές χώρες η προστασία της ιδιωτικής ζωής δεν αναγνωρίζεται ρητά από το Σύνταγμα. Τα δικαστήρια χώρων όπως οι Ηνωμένες Πολιτείες, η Ιρλανδία και η Ινδία, έχουν διαπιστώσει το δικαίωμα αυτό σε άλλες διατάξεις. Σε άλλες περιπτώσεις, διεθνείς συμφωνίες που αναγνωρίζουν το δικαίωμα της ιδιωτικής ζωής, όπως το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα και η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου, έχουν εγκριθεί σε νόμους.

Οι νόμοι για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων έχουν υιοθετηθεί σε όλο τον κόσμο. Οι στόχοι τους διαφέρουν από χώρα σε χώρα. Κάποιοι από τους νόμους προσπαθούν να διορθώσουν αδικίες του παρελθόντος, κάποιοι άλλοι επιδιώκουν την προώθηση του ηλεκτρονικού εμπορίου, προσπαθώντας να εξασφαλίσουν ένα ικανοποιητικό επίπεδο προστασίας, ώστε να επιτρέπεται το παγκόσμιο εμπόριο. Ανεξάρτητα από το στόχο, οι νόμοι προστασίας δεδομένων τείνουν

να συγκλίνουν γύρω από την αρχή ότι τα άτομα θα πρέπει να έχουν τον έλεγχο επί των προσωπικών τους πληροφοριών.²⁰⁹

Παρά το γεγονός ότι η έκφραση των απαιτήσεων προστασίας των δεδομένων ποικίλλει από χώρα σε χώρα, σχεδόν σε όλες τις χώρες, απαιτείται ότι οι προσωπικές πληροφορίες πρέπει να:

- Λαμβάνονται με νόμιμο και θεμιτό τρόπο
- Χρησιμοποιούνται μόνο για το συγκεκριμένο σκοπό για τον οποίο έχουν συλλεγεί
- Είναι συναφή και όχι υπερβολικά για το σκοπό για τον οποίο έχουν συλλεγεί
- Είναι ακριβή και ενημερωμένα
- Φυλάσσονται με ασφάλεια
- Καταστρέφονται όταν ο σκοπός για τον οποίο έχουν συλλεγεί έχει ολοκληρωθεί

Υπάρχουν επί του παρόντος πολλά σημαντικά μοντέλα για την προστασία της ιδιωτικής ζωής. Σε ορισμένες χώρες, τα διάφορα μοντέλα χρησιμοποιούνται ταυτόχρονα. Το κανονιστικό μοντέλο που υιοθετήθηκε από την Ευρώπη, την Αυστραλία, και τον Καναδά είναι ότι το κράτος θα πρέπει να ορίζει και να εφαρμόζει μια ολοκληρωμένη νομοθεσία ώστε να παρέχει στον πολίτη προστασία, τόσο στον κρατικό τομέα, όσο και στον ιδιωτικό. Ο υπάλληλος, γνωστός ως Επίτροπος, διαμεσολαβητής ή γραμματέας, παρακολουθεί τη συμμόρφωση με τη νομοθεσία και διεξάγει έρευνες για εικαζόμενες παραβάσεις. Σε ορισμένες περιπτώσεις, ο υπάλληλος μπορεί να προσφύγει κατά του δράστη. Ο υπάλληλος είναι επίσης υπεύθυνος για τη δημόσια εκπαίδευση και τη διεθνή συνεργασία στον τομέα της προστασίας και της μεταφοράς των δεδομένων. Αυτό είναι το προτιμώμενο μοντέλο για τις περισσότερες χώρες, για τη θέσπιση νομοθεσίας περί προστασίας δεδομένων. Είναι, επίσης, το μοντέλο που ευνοείται από την Ευρώπη για να εξασφαλιστεί η συμμόρφωση με το νέο καθεστώς προστασίας των δεδομένων του. Ωστόσο, οι αρμοδιότητες των επιτροπών

²⁰⁹ www.gilc.org/privacy/survey/intro.html (28/04/2013)

διαφέρουν σε μεγάλο βαθμό και πολλοί αναφέρουν μια σοβαρή έλλειψη πόρων για την επιβολή του νόμου.

Ορισμένες χώρες, όπως οι Ηνωμένες Πολιτείες έχουν αποφύγει γενικών κανόνων προστασίας των δεδομένων, χρησιμοποιώντας συγκεκριμένους τομεακούς νόμους. Σε τέτοιες περιπτώσεις, η επιβολή επιτυγχάνεται μέσω μιας σειράς μηχανισμών. Η έλλειψη νομικής προστασίας για τις γενετικές πληροφορίες στις ΗΠΑ είναι ένα εντυπωσιακό παράδειγμα των περιορισμών της. Σε άλλες χώρες, οι τομεακές νομοθεσίες που χρησιμοποιούνται για να ολοκληρώσουν τη νομοθεσία, παρέχοντας πιο λεπτομερή προστασία για ορισμένες κατηγορίες πληροφοριών, όπως αρχεία της αστυνομίας ή τα αρχεία της καταναλωτικής πίστης.²¹⁰

Η προστασία των δεδομένων μπορεί επίσης να επιτευχθεί μέσω διαφόρων μορφών αυτορρύθμισης, στην οποία, εταιρείες και φορείς του κλάδου, θεσπίζουν κώδικες πρακτικής. Ωστόσο, το αποτέλεσμα αυτών των προσπαθειών υπήρξε απογοητευτικό, με ελάχιστη ή καμία απόδειξη ότι οι στόχοι των κωδικών πληρούνται. Η επάρκεια και η εκτέλεση είναι το μεγάλο πρόβλημα με αυτές τις προσεγγίσεις. Χώρες όπως Ηνωμένες Πολιτείες, και την Αυστραλία παρέχουν μόνο αδύναμη προστασία και έχουν έλλειψη επιβολής του νόμου.

Ακόμη και με την έγκριση της νομικής και άλλες εγγυήσεις, παραβιάσεις της ιδιωτικής ζωής εξακολουθούν να προκαλούν ανησυχία. Σε πολλές χώρες, οι νόμοι δεν συμβαδίζουν με την τεχνολογία, και αφήνουν σημαντικά κενά στην προστασία. Σε άλλες χώρες, οι υπηρεσίες επιβολής του νόμου και πληροφοριών έχουν σημαντικές εξαιρέσεις. Τέλος, η έλλειψη επαρκούς εποπτείας και της επιβολής του νόμου, η απλή παρουσία ενός νόμου δεν μπορεί να παρέχει επαρκή προστασία. Υπάρχουν εκτεταμένες παραβιάσεις των νόμων που αφορούν την εποπτεία των επικοινωνιών, ακόμη και στις πιο δημοκρατικές χώρες

Με την ανάπτυξη της εμπορικά διαθέσιμη τεχνολογίας συστήματα που βασίζονται, προστασία της ιδιωτικής ζωής έχουν γίνει προσβάσιμα τους. Οι χρήστες του διαδικτύου μπορούν να χρησιμοποιούν μια σειρά από προγράμματα και συστήματα που θα εξασφαλίζουν σε ένα βαθμό την προστασία της ιδιωτικής ζωής και της

²¹⁰ www.gilc.org/privacy/survey/intro.html (28/04/2013)

ασφάλειας των επικοινωνιών. Πάνω απ' όλα όμως είναι στην ευχέρεια του καθενός μας, για το ποια από τα στοιχεία μας θα αφήσουμε να διαρρεύσουν στο διαδίκτυο. Επίσης, θα πρέπει όλοι μας να χρησιμοποιούμε τα στοιχεία των άλλων, όταν αυτό επιτρέπεται, με σεβασμό στην αξία της ιδιωτικής ζωής, χωρίς να προσβάλουμε την προσωπικότητα και γενικά, το άτομο που αφορούν οι πληροφορίες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Αλεξανδροπούλου-Αιγυπτιάδου Ε., Νομική διασφάλιση του απορρήτου των κινητών επικοινωνιών, Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας, 2008.
2. Αλεξανδροπούλου-Αιγυπτιάδου Ε., Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου, 2005, Αρμ59.
3. Αλεξανδροπούλου-Αιγυπτιάδου Ε., Ζητήματα από το δίκαιο Πληροφορικής, 2002.
4. Αρμαμέντου Π.- Σωτηρόπουλος Β., Ερμηνεία Ν.2472/1997, 2005 .
5. Βαθρακοκοίλη Β., Ερμηνεία Αστικού Κώδικα, Τόμος Α, 2001.
6. Βασιλάκη Ειρήνη, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993.
7. Γέροντα Α., Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, 2002.
8. Γιαννόπουλος Γ., Ροή πληροφοριών στο διαδίκτυο, τεχνολογία και νομικές ρυθμίσεις, 2002.
9. Δαγτόγλου Π.Δ., Συνταγματικό Δίκαιο, Ατομικά και Κοινωνικά Δικαιώματα, 2005.
10. Ιγγλεζάκης Ι., Εισαγωγή στο δίκαιο της πληροφορικής, 2007.
11. Ιγγλεζάκης Ι., Ευαίσθητα προσωπικά δεδομένα, 2003.
12. Καΐσης Α.Γ. - Ν.Α.Μ. Παρασκευόπουλος, Προστασία Προσωπικών Δεδομένων, 2001.

13. Καράκωστα Ι, Το δίκαιο του Ίντερνετ (Νομική αντιμετώπιση του διαδικτύου), ΝοΒ,1998.
14. Καράκωστας Ι., Προστασία της ιδιωτικότητας στην κοινωνία της Πληροφορίας, 2004.
15. Κυριακόπουλος Γ., Ασφάλεια και επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Οι ρυθμίσεις του Συμβουλίου της Ευρώπης, ΔτΑ, 11/2001.
16. Λάζος Γ., Πληροφορική και έγκλημα, 2001.
17. Μαντζούφα Π., Η διακινδύνευση στην κοινωνία της πληροφορίας και η προστασία των προσωπικών δεδομένων, 2007.
18. Μαρίνος Α., Ηλεκτρονικοί υπολογιστές και το δίκαιο: informatique juridique, 1980.
19. Μαρίνος Α., Ηλεκτρονικοί υπολογιστές και το δίκαιο, δευτ. έκδοση, 1991.
20. Μαυριά Κ., Το συνταγματικό δικαίωμα του ιδιωτικού βίου, 1982.
21. Μήτρου Λίλιαν, Το δίκαιο στην κοινωνία της πληροφορίας, 2003.
22. Νουσκάλης Γ., Ποινική προστασία προσωπικών δεδομένων: η νομολογιακή συμβολή στην ερμηνεία βασικών όρων, β' εκδ., 2007.
23. Παπακωνσταντίνου Ε., Νομικά Θέματα Πληροφορικής, 2006.
24. Σημίτης Σ., Ηλεκτρονικοί υπολογιστές και νομική παιδεία. Προϋποθέσεις, επιπτώσεις, προοπτικές, Πληροφορική και δίκαιο, 1987.
25. Σωτηρόπουλος Β., Η συνταγματική προστασία των προσωπικών δεδομένων, 2006.
26. Σωτηρόπουλος Β., Η πρόσβαση στη δημόσια πληροφορία και η προστασία προσωπικών δεδομένων, Digesta, 2005.
27. Τουντόπουλος Β, Η διασύνδεση αρχείων στον.2472/1997,ΝοΒ, 1999.
28. Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων, ΔΕΕ, 1999.

29. Τουντόπουλος Β., Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων, ΤοΣ, 1999.
30. Χριστοδούλου Κ., Προστασία της προσωπικότητας και της συμβατικής ελευθερίας στα κοινωφελή δίκτυα, 2007.

ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Bygrave L. A., Privacy Protection in a Global Context – A Comparative Overview. Scandinavian Studies in Law, 2004.
2. Cate F., Privacy and Telecommunications, 1998.
3. Chemerinsky E., Constitutional law: principles and policies, 1997.
4. Gutwirth Serge, Privacy and the information age, 2002.
5. Warren Samuel and Brandeis Luis, The right to privacy, Harvard Law Review, vol. IV, 1980.

ΠΗΓΕΣ ΔΙΑΔΙΚΤΥΟΥ

1. www.acma.gov.au/WEB/HOMEPAGE/PC=HOME (09/04/2013)
2. www.acma.gov.au/WEB/STANDARD/pc=PC_310521 (09/04/2013)
3. www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf (09/04/2013)
4. www.alrc.gov.au/publications/19.%20Consent/background (09/04/2013)

5. www.alrc.gov.au/publications/5.%20The%20Privacy%20Act%3A%20Name,%20Structure%20and%20Objects/overview-privacy-act (09/04/2013)
6. www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/what-%E2%80%98personal-information%E2%80%99 (09/04/2013)
7. www.aspe.hhs.gov/datacncl/niiprivp.htm (08/02/2013)
8. www.athens.usembassy.gov/faq-gr.html(08/02/2013)
9. www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/ (09/04/2013)
10. www.austlii.edu.au/itlaw/articles/Waters_Interception.html (09/04/2013)
11. www.bfd.bund.de/information/gesetze.html
12. www.bfdi.bund.de (14/02/2013)
13. www.cnil.fr/english/topics/blacklists/accessible/non/ (10/04/2013)
14. www.cnil.fr/english/topics/human-resources/ (10/04/2013)
15. www.cnil.fr/english/topics/regulating-biometrics/ (10/04/2013)
16. www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (10/04/2013)
17. www.csa.ca/cm/ca/en/privacy-code (12/04/2013)
18. www.cylaw.org/nomoi/arith/2012_1_51.pdf (11/04/2013)
19. www.cylaw.org/nomoi/enop/non-ind/2004_1_112/index.html (11/04/2013)
20. www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.CY (11/04/2013)
21. [www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/37D957C789729A48C2257A15004BA5A3/\\$file/51%28I%29-2012.pdf?OpenElement](http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/37D957C789729A48C2257A15004BA5A3/$file/51%28I%29-2012.pdf?OpenElement) (11/04/2013)
22. [www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B708D98FB15F8D09C2256D9B0032AE61/\\$file/138%28I%29-2001&37%28I%29-2003&105%28I%29-2012_el.pdf?OpenElement](http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B708D98FB15F8D09C2256D9B0032AE61/$file/138%28I%29-2001&37%28I%29-2003&105%28I%29-2012_el.pdf?OpenElement) (11/04/2013)

23. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/EBB3D2DFD991CCC4C22572A60032B214?OpenDocument (11/04/2013)
24. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/duties_gr/duties_gr?OpenDocument (11/04/2013)
25. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/responsib_gr/responsib_gr?OpenDocument (11/04/2013)
26. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/rights_gr/rights_gr?OpenDocument (11/04/2013)
27. www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/spam_gr/spam_gr?OpenDocument (11/04/2013)
28. www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/%CE%9DOMOTHESIA%20PROSOPIKA%20DEDOMENA_GREEK/3471_06_MAY2012FINAL.PDF (08/02/2013)
29. www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#2 (08/02/2013)
30. www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#9 (08/02/2013)
31. www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#11 (08/02/2013)
32. www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#13 (08/02/2013)
33. www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#14 (08/02/2013)
34. www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#15 (08/02/2013)
35. www.dsanet.gr/Epikairothta/Nomothesia/n3471_06.htm (08/02/2013)
36. www.egkykloi.moec.gov.cy/Data/dde2918b.pdf (11/04/2013)

37. www.epic.org/privacy/1974act/ (08/02/2013)
38. www.et.gr/index.php?option=com_wrapper&view=wrapper&Itemid=108&lang=el
39. www.eur-lex.europa.eu/LexUriServ.do?uri=CELEX:32006L0024:el:HTML
(14/04/2013)
40. www.eur-lex.europa.eu/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EL:PDF
(14/04/2013)
41. www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dt/830/830120/830120el.pdf (08/02/2013)
42. www.export.gov/safeharbor (08/02/2013)
43. www.export.gov/safeharbor/eu/eg_main_018476.asp (08/02/2013)
44. www.fourthamendmentsummaries.com/ (08/02/2013)
45. www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (08/02/2013)
46. www.ftc.gov/reports/privacy2000/privacy2000.pdf (08/02/2013)
47. www.garantepriacy.it/documents/10160/10704/Data+protection+code
(14/04/2013)
48. www.garantepriacy.it/home_en (14/04/2013)
49. www.garantepriacy.it/home_en/italian-legislation (14/04/2013)
50. www.gilc.org/privacy/survey/intro.html (28/04/2013)
51. www.gov.uk/make-a-freedom-of-information-request/organisations-you-can-request-information-from (10/04/2013)
52. www.groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_war2.html
53. www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-9a/ (08/04/2013)

54. www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-5a/ (08/04/2013)
55. www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/article-105/ (08/04/2013)
56. www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00218.html (12/04/2013)
57. www.ico.org.uk/what_we_cover (08/04/2013)
58. www.ics.uci.edu/~kobsa/privacy/Italian-privacy-law.html (14/04/2013)
59. www.ipandit.practicallaw.com/9-502-4794 (14/04/2013)
60. www.itic.org (08/02/2013)
61. www.itu.int/osg/spu/spam/legislation/legislation_italy_old.html (14/04/2013)
62. www.iuscomp.org/gla/statutes/GG.htm (09/02/2013)
63. www.jisclegal.ac.uk/dataprotection/dataprotection.htm (10/04/2013)
64. www.law.cornell.edu/uscode/text/5/552a&usg=ALkJrhiUJhA16pMDtQR1H_YUsJdYMgxRIQ(08/02/2013)
65. www.law.uts.edu.au/comslaw/factsheets/privacy.html (09/04/2013)
66. www.lawhandbook.org.au/handbook/ch21s05s02.php (09/04/2013)
67. www.laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html (12/04/2013)
68. www.laws-lois.justice.gc.ca/eng/acts/P-21/page-15.html (12/04/2013)
69. www.laws-lois.justice.gc.ca/eng/acts/P-21/page-2.html (12/04/2013)
70. www.laws-lois.justice.gc.ca/eng/acts/P-21/page-3.html (12/04/2013)
71. www.laws-lois.justice.gc.ca/eng/acts/P-8.6/page-2.html (12/04/2013)
72. www.laws-lois.justice.gc.ca/eng/acts/P-8.6/page-3.html (12/04/2013)
73. www.laws-lois.justice.gc.ca/eng/acts/P-8.6/page-7.html (12/04/2013)

74. www.laws-lois.justice.gc.ca/eng/const/page-15.html#h-44 (12/04/2013)
75. www.ldlaw.com.cy/services/dataprotection.htm (11/04/2013)
76. www.legal-dictionary.thefreedictionary.com/Fourth+Amendment (08/02/2013)
77. www.legislation.gov.uk/ukpga/2000/36/part/VII (10/04/2013)
78. www.legislation.gov.uk/ukpga/2000/36/section/18 (10/04/2013)
79. www.legislation.gov.uk/ukpga/2000/36/section/68 (10/04/2013)
80. www.legislation.gov.uk/ukpga/2000/36/section/80 (10/04/2013)
81. www.mfa.gov.cy/mfa/mfa2006.nsf/constitution_gr/constitution_gr (11/04/2013)
82. www.mondaq.com/australia/x/230850/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Australia (09/04/2013)
83. www.mondaq.com/x/230888/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Cyprus (11/04/2013)
84. www.ntia.doc.gov/legacy/ntiahome/privacy/mail/disk/irsgcom.html
(08/02/2013)
85. www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html (08/02/2013)
86. www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html (09/04/2013)
87. www.oecd.org/sti/interneteconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2
88. www.out-law.com/page-413 (08/04/2013)
89. www.parl.gc.ca/Content/LOP/ResearchPublications/prb0585-e.htm (12/04/2013)
90. www.parl.gc.ca/HousePublication.aspx?Pub=Bill&Doc=c-6_4%Language=&Mode=1&Parl=36&Ses=2&File=16 (12/04/2013)
91. www.priv.gc.ca/information/02_05_d_08_e.asp (12/04/2013)

92. www.priv.gc.ca/leg_c/legislation/02_06_07_e.asp (12/04/2013)
93. www.privacy.gov.au/materials/types/infosheets/view/6541 (09/04/2013)
94. www.privacy.gov.au/materials/types/infosheets/view/6583 (09/04/2013)
95. www.privacy.it/privacypcode-en.html (14/04/2013)
96. www.privacyalliance.org/ (08/02/2013)
97. www.privacyinternational.org/reports/germany/i-legal-framework (09/04/2013)
98. www.privacysense.net/10-privacy-principles-of-pipeda/ (12/04/2013)
99. www.privereal.org/content/dp/cyprus.php (11/04/2013)
100. www.privereal.org/content/dp/italy.php (14/04/2013)
101. www.services.whitecase.com/wcu/getdoc.aspx?pid=4&cid=2
(09/04/2013)
102. www.services.whitecase.com/wcu/getdoc.aspx?pid=4&cid=2
(09/04/2013)
103. www.services.whitecase.com/wcu/getdoc.aspx?pid=4&cid=2
(09/04/2013)
104. www.soas.ac.uk/infocomp/dpa/policy/overview (08/04/2013)
105. www.soas.ac.uk/infocomp/dpa/policy/overview (08/04/2013)
106. www.thedma.org/services/privacy/ (08/02/2013)