ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα μεταπτυχιακών σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ της
Μαργαρίτας Σταθοπούλου (Α.Μ: ΜΔΙ 2242)

ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΗΔΗ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ /ΑΣΦΑΛΕΙΑ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ

Επιβλέπουσα Καθηγήτρια
Λίλιαν Μήτρου

Πειραιάς, Νοέμβριος 2024

“Design is not just what it looks like and feels like.

Design is how it works!”

SteveJobs

ΠΕΡΙΛΗΨΗ

Η μεταπτυχιακή διπλωματική εργασία εξετάζει την έννοια της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Εστιάζει στις θεμελιώδεις αρχές Privacy by Design και Privacy by Default, που στοχεύουν στην ενσωμάτωση της προστασίας της ιδιωτικής ζωής από τα αρχικά στάδια ανάπτυξης των συστημάτων ή υπηρεσιών. Στην συνέχεια, εμβαθύνει στις νομικές διαστάσεις του άρθρου 25 του ΓΚΠΔ και αναλύει ορισμένες από τις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας. Παρουσιάζει, επίσης, παραδείγματα προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού από τον ψηφιακό κόσμο. Ακολούθως, εξετάζει την ευρωπαϊκή και εθνική διάσταση της προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Τέλος, παρουσιάζει ορισμένες αδυναμίες και προκλήσεις τους άρθρου 25 ΓΚΠΔ και καταλήγει σε ορισμένα συμπεράσματα.

ABSTRACT

The thesis examines the meaning of Data Protection by Design and by Default, according to the General Data Protection Regulation (GDPR). It focuses on the fundamental principles of Privacy by Design and Privacy by Default, which aim to integrate privacy protection from the initial stages of development of systems or services. It, then, delves into the legal dimensions of Article 25 of the GDPR and analyses some of the Privacy Enhancing Technologies. It, also, gives some examples of Data Protection by Design and By Default by the technology world. Additional, it discusses the European and national dimension of Data Protection by Design and by Default. Finally, it presents some weaknesses and challenges of Article 25 GDPR and draws some conclusions.

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Το δικαίωμα της προστασίας της ιδιωτικότητας, ως απόρροια του συνταγματικού δικαιώματος στην ελεύθερη ανάπτυξη της προσωπικότητας, συνδέεται άμεσα με τον έλεγχο της αξιοπρέπειας και της ζωής κάθε ανθρώπου, αποτελώντας ένα θεμελιώδες ανθρώπινο δικαίωμα, το οποίο αναγνωρίζεται και κατοχυρώνεται σε διεθνείς συμβάσεις, συνταγματικές διατάξεις, αλλά και σε πλήθος δικαστικών αποφάσεων. Το εν λόγω δικαίωμα περιλαμβάνει, μεταξύ άλλων, μία εδαφική διάσταση, η οποία σχετίζεται με την προστασία από την πρόσβαση στον προσωπικό χώρο ενός ατόμου, είτε αυτός ο χώρος είναι η κατοικία του ή ο χώρος όπου εργάζεται, είτε ακόμη και ο στενός δημόσιος χώρος που περιβάλλει ένα φυσικό πρόσωπο.[1] Εντός αυτής της ιδιωτικής σφαίρας, το άτομο μπορεί να διαμορφώσει τις πεποιθήσεις του, από τις οποίες αυτοπροσδιορίζεται και να αναπτύξει την προσωπικότητα του ελεύθερα. Η προστασία της ιδιωτικής ζωής κατοχυρώνεται στο άρθρο 9 παρ. 1 εδ. β' του Συντάγματος, που ορίζει ότι «*η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη*».[2] Με την αναθεώρηση του Συντάγματος, το 2001 προστέθηκε το άρθρο 9^{A} που προστατεύει τα προσωπικά δεδομένα και κατοχυρώνει το δικαίωμα της πληροφοριακής αυτοδιάθεσης ή πληροφοριακού αυτοκαθορισμού.[3] Έτσι, κάθε άνθρωπος έχει το δικαίωμα να μην καθίσταται πληροφοριακό αντικείμενο, αλλά να έχει την δυνατότητα να προσδιορίζει ο ίδιος ποιες πληροφορίες θα γνωστοποιηθούν στο περιβάλλον του. Είναι αξιοσημείωτο ότι, δεν αποτελούν η πληροφορία και τα δεδομένα το προστατευτέο αγαθό του άρθρου 9^{A} του Συντάγματος, αλλά η αυτονομία του ατόμου.[4]

Επισημαίνεται, επίσης, ότι το εν λόγω άρθρο δεν συνιστά απλώς μια επανάληψη των άρθρων του Συντάγματος που προστατεύουν την προσωπικότητα και την

[1] Κανέλλος,2021,σ.107
[2] Λαζαράκος,2017,σ.229
[3] Δαντόγλου,2012,σ.274
[4] Παναγοπούλου,2023,σ.8

ιδιωτική ζωή, αλλά έχει αυτοτελή και ιδιαίτερη αξία, καθώς προστατεύει κατά κύριο λόγο μια πτυχή της προσωπικότητας του ανθρώπου που βρίσκεται υπό διακινδύνευση λόγω της ραγδαίας ανάπτυξης της τεχνολογίας. Γι' αυτό το λόγο και το άρθρο 9ΑΣ επικεντρώνεται ιδίως στα ηλεκτρονικά μέσα.[5]

Ωστόσο, το δικαίωμα προστασίας των προσωπικών δεδομένων δεν εμφανίστηκε για πρώτη φορά το 2001, αλλά αναπτύχθηκε το 1983 από το Ομοσπονδιακό Συνταγματικό Δικαστήριο της Γερμανίας, ως το δικαίωμα του κάθε ανθρώπου να αποφασίζει ο ίδιος/η, ποιος, τι, από πού, και για ποιο λόγο και σκοπό θα γνωρίζει για αυτόν/ην.[6] Επίσης, το εν λόγω δικαίωμα απολαμβάνει διεθνούς προστασίας, καθώς κατοχυρώνεται στο άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (εφεξής ΕΣΔΑ), ως ιδιαίτερη πτυχή του εκεί κατοχυρωμένου δικαιώματος στην ιδιωτική ζωή,[7] με το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων να έχει αναμφισβήτητα αναγνωρίσει την προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού ως απαίτηση βάσει του άρθρου 8 της ΕΣΔΑ.[8]

Περαιτέρω, στο άρθρο 7 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (εφεξής ΧΘΔΕΕ) κατοχυρώνεται το θεμελιώδες δικαίωμα της προστασίας της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, ενώ στο άρθρο 8 του ΧΘΔΕΕ κατοχυρώνεται ρητώς το δικαίωμα προστασίας των προσωπικών δεδομένων. Το άρθρο 7 ΧΘΔΕΕ μπορεί να αποτελεί την πηγή από την οποία προέκυψε το άρθρο 8 ΧΘΔΕΕ[9], ωστόσο, από τον Χάρτη επιβάλλεται η αυτόνομη θεώρησή των δύο δικαιωμάτων. Επίσης, και το άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης το οποίο αποτελεί ενιαία νομική βάση για την υιοθέτηση μέτρων σχετικών με την προστασία των προσωπικών δεδομένων σε όλους τους τομείς του δικαίου της Ένωσης[10],κατοχυρώνει το δικαίωμα της προστασίας προσωπικών δεδομένων στην έννομη τάξη της

[5]Οπ., ,σ.7
[6]Λαζαράκος, 2017,σ.245
[7]Παναγοπούλου,2023,σ.183
[8] Michelakaki and Barros Vale,2023, p.5
[9]Παπαδημητρίου,2015,σ.87
[10]Ο.π.,σ.102

Ευρωπαϊκής Ένωσης, με ένα μέρος των διατάξεων του εν λόγω άρθρου να περιλαμβάνονται, ήδη στο άρθρο 8 του ΧΘΔΕΕ.[11]

Είναι αξιοσημείωτο ότι, η ιδιωτικότητα και η προστασία προσωπικών δεδομένων μοιράζονται έναν κοινό σκοπό, ο οποίος δεν είναι άλλος, από την προστασία της αυτονομίας κάθε άτομού, ως προϋπόθεση συμμετοχής του σε μία δημοκρατική κοινωνία.[12]Η παρουσία των ατόμων στον κυβερνοχώρο τείνει να αυξάνει ολοένα και περισσότερο την ανάγκη προστασίας τους δικαιώματος της ιδιωτικότητας τους, και σε συνδυασμό με το συνεχώς εξελισσόμενο ψηφιακό τοπίο η ευρωπαϊκή νομοθεσία για την προστασία της ιδιωτικότητας, στοχεύει στη διασφάλιση του δικαιώματος της «πληροφοριακής αυτοδιάθεσης» του ατόμου. Το δικαίωμα αυτό συνίσταται στην ικανότητα του ατόμου να ελέγχει την διαχείριση κυκλοφορίας των πληροφοριών που το αφορούν, καθώς και να διαχωρίζει τις δημόσιες διαθέσιμες πληροφορίες από τις ιδιωτικές, η κοινοποίηση των οποίων σε συγκεκριμένους αποδέκτες εξαρτάται από τη δική του βούληση και τη συγκατάθεση του ατόμου. [13] Επομένως, το δικαίωμα στην προστασία των προσωπικών δεδομένων αποδίδει στο άτομο την εξουσία να ελέγχει τις πληροφορίες που το αφορούν, ως εκδήλωση του πληροφοριακού αυτοπροσδιορισμού.

Η παρούσα διπλωματική εργασία εξετάζει την έννοια της προστασίας των προσωπικών δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, στηριζόμενη στις θεμελιώδης αρχές της Privacy by Design και Privacy by Default, οι οποίες αποσκοπούν στη διασφάλιση της ιδιωτικότητας σε όλα τα στάδια του κύκλου ζωής ενός συστήματος ή μιας υπηρεσίας. Εν συνεχεία, η εργασία εμβαθύνει στις νομικές διαστάσεις του άρθρου 25 ΓΚΠΔ και αναλύει την έννοια των τεχνολογιών ενίσχυσης της ιδιωτικότητας, καθώς και μερικά από τα τεχνικά και οργανωτικά μέτρα που ενισχύουν την ασφάλεια της επεξεργασίας των προσωπικών δεδομένων. Μετέπειτα, αναλύονται δύο παραδείγματα προστασίας προσωπικών δεδομένων από τον σχεδιασμό και εξ ορισμού, όπου και τα δύο απορρέουν από

[11]Φαραντούρης,2012,σ.217
[12]Μήτρου,2024,,σ.15
[13]Κανέλλος,2021,σ.110

τον ψηφιακό κόσμο. Ακολούθως, αναδεικνύονται οι διαστάσεις εφαρμογής της προστασίας δεδομένων από τον σχεδιασμό, σε ευρωπαϊκό και εθνικό επίπεδο και αναλύονται ορισμένες αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής ΑΠΔΠΧ). Τέλος, η εργασία ολοκληρώνεται με την ανάδειξη και την καταγραφή ορισμένων αδυναμιών και προκλήσεων που απορρέουν από το άρθρο 25 του Γενικού Κανονισμού Προστασίας Δεομένων (εφεξής ΓΚΠΔ).

ΚΕΦΑΛΑΙΟ 1ο ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ

1.1 Έννοια της Προστασίας της Ιδιωτικής Ζωής από τον σχεδιασμό (Privacy by Design)

Η ιδέα της «Προστασίας της Ιδιωτικής ζωής από το Σχεδιασμό» δεν είναι μια σύγχρονη ιδέα, απόρροια της τεχνολογικής εξέλιξης, αλλά υπάρχει εδώ και περισσότερα από 20 χρόνια. Ο όρος Privacy by Design (εφεξής PbD) αναπτύχθηκε στα μέσα της δεκαετίας του '90 από την Ann Cavoukian, πρώην Επίτροπο, αρμόδια για ζητήματα Πληροφοριών & Προστασίας της Ιδιωτικής Ζωής στο Οντάριο του Καναδά και το 2010, αναγνωρίστηκε διεθνώς στη 32η Διεθνής Διάσκεψη των Επιτρόπων Προστασίας Δεδομένων και Ιδιωτικότητας που έλαβε χώρα στην Ιερουσαλήμ. Το *«Ψήφισμα για την προστασία της ιδιωτικής ζωής από τον σχεδιασμό»* που εγκρίθηκε από την εν λόγω Διάσκεψη, αποτελεί ορόσημο για την αναγνώριση του PbD ως βασικού συστατικού στοιχείου της θεμελιώδους προστασίας της ιδιωτικής ζωής.[14] Η Διάσκεψη αναγνώρισε, επίσης, την καίρια σημασία της ενσωμάτωσης των αρχών απορρήτου στις διαδικασίες λειτουργίας, διαχείρισης και σχεδιασμού των συστημάτων, αποσκοπώντας στην επίτευξη ενός ολοκληρωμένου πλαισίου προστασίας δεδομένων. Κάλεσε, επίσης, τις Αρχές Προστασίας Δεδομένων κάθε κράτους μέλους να εργαστούν με κατεύθυνση τη προώθηση της προστασίας της ιδιωτικής ζωής μέσω σχεδιασμού στο νομοθετικό πλαίσιο στις αντίστοιχες δικαιοδοσίες τους. Τέλος ενθάρρυνε και υποστήριξε την υιοθέτηση των θεμελιωδών αρχών προστασίας προσωπικών δεδομένων, όπως ορίζονται από την Ann Cavoukian, ζήτημα που θα αναλυθεί αμέσως παρακάτω.

1.2 Οι επτά (7) θεμελιώδεις αρχές της Privacy by Design

Η εφαρμογή της προστασίας της ιδιωτικής ζωής μέσω σχεδιασμού σημαίνει να εστιάζουμε και να ανταποκρινόμαστε στις ακόλουθες 7 θεμελιώδεις αρχές, οι οποίες αποτελούν και την ουσία του PbD.[15] Οι εν λόγω αρχές διατυπώνουν ένα σύνολο στόχων για να επιτευχθεί η ενσωμάτωση των παραμέτρων προστασίας

[14]Schwaab, 2010,p.1
[15]Cavoukian, 2010, p. 249

της ιδιωτικής ζωής στις προδιαγραφές σχεδιασμού διαφόρων τεχνολογικών συστημάτων, στις επιχειρηματικές πρακτικές και στις δικτυακές υποδομές αποτελώντας, δε, το θεμέλιο για περαιτέρω έρευνα.[16] Είναι, όμως γεγονός ότι για να επιτευχθεί μια ενσωμάτωση της προστασίας των δεδομένων στον σχεδιασμό συστημάτων πληροφορικής, η οποία θα είναι ρεαλιστική, απαιτείται ένας περαιτέρω καθορισμός τόσο λειτουργικών απαιτήσεων όσο και στρατηγικών.[17]

1.2.1Πρόληψη, όχι Αντίδραση: Αποτροπή, όχι Επανόρθωση

Η προσέγγιση της προστασίας της ιδιωτικής ζωής μέσω σχεδιασμού χαρακτηρίζεται από προληπτικά και όχι αντιδραστικά μέτρα. Περιλαμβάνει την πρόβλεψη και αποτροπή γεγονότων που παραβιάζουν την ιδιωτικότητα πριν αυτά συμβούν. Οποιοδήποτε σύστημα, διαδικασία ή υποδομή που χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα είναι αναγκαίο να σχεδιαστεί από την αρχή λαμβάνοντας υπόψιν ενδεχόμενους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, όπου αναφέρονται τα δεδομένα, αποσκοπώντας στην ελαχιστοποίηση των εν λόγω κινδύνων, προτού αυτά οδηγήσουν στην πρόκληση πραγματικής ζημιάς. Άρα, η λογική επί της οποίας στηρίζεται το PbD είναι η υιοθέτηση προδραστικών και όχι αντιδραστικών μέτρων, καθώς και η διαρκής υιοθέτηση ισχυρών πρακτικών προστασίας της ιδιωτικότητας. Επιπλέον, μείζονος σημασίας είναι η ανάπτυξη συστηματικών μεθόδων που στοχεύουν, τόσο στην έγκαιρη αναγνώριση και στον αποτελεσματικό εντοπισμό πρακτικών και διαδικασιών που εγγυώνται την προστασία της ιδιωτικής ζωής και την ασφάλεια της ιδιωτικότητας, όσο και στην πρόληψη των επιπτώσεων πριν παρουσιαστούν. Άρα το PbD αποφεύγει την «πολιτική της διόρθωσης»[18], αλλά αντιθέτως, στοχεύει στην εξ αρχής αποτροπή της πραγματοποίηση των επιπτώσεων τους.

[16]Information and Privacy Commissioner of Ontario,2018,pp.1-2
[17]Λουκάς,2019, σελ.46-51
[18]Cavoukian,2011,pp.1-2

1.2.2 Προστασία Δεδομένων ως προεπιλεγμένη ρύθμιση

Η αρχή του PbD αποσκοπεί στην επίτευξη του μέγιστου βαθμού προστασίας της ιδιωτικότητας, εξασφαλίζοντας ότι τα προσωπικά δεδομένα προστατεύονται αυτόματα σε οποιοδήποτε σύστημα πληροφορικής, χωρίς να απαιτείται καμία ενέργεια εκ μέρους του υποκειμένου των δεδομένων για την προστασία των προσωπικών του δεδομένων και του απορρήτου του, καθώς η προστασία είναι ενσωματωμένη στο σύστημα, από προεπιλογή (by default)[19].Ειδικότερα, η αρχή του PbD υπό το πρίσμα του «Privacy by Default» διαπνέεται από την εξειδίκευση του σκοπού, ο οποίος θα πρέπει να είναι σαφής, σχετικός και ανάλογος των περιστάσεων επεξεργασίας. Οι σκοποί για τους οποίους τα δεδομένα συλλέγονται, χρησιμοποιούνται, διατηρούνται και γνωστοποιούνται σε τρίτους, θα πρέπει να κοινοποιούνται στο υποκείμενο των δεδομένων, προκειμένου εκείνο με τη σειρά του να είναι ενήμερο για τους εν λόγω σκοπούς. Η ενημέρωση αυτή θα πρέπει να πραγματοποιείται είτε πριν είτε κατά τη στιγμή της συλλογής των δεδομένων. Επιπλέον, η συλλογή των προσωπικών δεδομένων πρέπει να είναι νόμιμη, δίκαιη και να περιορίζεται στις πληροφορίες που είναι απολύτως αναγκαίες και απαραίτητες για την υλοποίηση καθορισμένων σκοπών, ενώ στην περίπτωση που η εν λόγω συλλογή μπορεί να οδηγήσει στην ταυτοποίηση και στην σύνδεση με συγκεκριμένο πρόσωπο θα πρέπει να περιοριστεί στο ελάχιστο.[20] Τέλος, τα προσωπικά δεδομένα θα πρέπει να αποθηκεύονται μόνο για όσο χρονικό διάστημα είναι απολύτως απαραίτητο για την εκπλήρωση των σκοπών της επεξεργασίας, για τους οποίους το υποκείμενο των δεδομένων έχει ενημερωθεί και συναινέσει, και σε δεύτερο χρόνο να καταστρέφονται με ασφάλεια.

[19] ο.π
[20] AEPD, 2019, p.8

1.2.3 Ιδιωτικότητα ενσωματωμένη από το σχεδιασμό

Η Ιδιωτικότητα ενσωματώνεται στα στάδια της ανάπτυξης του σχεδιασμού και της αρχιτεκτονικής των συστημάτων πληροφορικής. [21] Δεν είναι ένα στοιχείο που προστίθεται, αργότερα, σε μια προϋπάρχουσα οντότητα (add- ons).[22] Η εν λόγω αρχή έχει ως αποτέλεσμα ότι η προστασία της ιδιωτικότητας αποτελεί βασικό συστατικό για τη λειτουργία του συστήματος και συνιστά ένα αναπόσπαστό στοιχείο του, δίχως, όμως να μειώνεται η λειτουργικότητα του.[23]

1.2.4 Πλήρης λειτουργικότητα : Θετικό άθροισμα όχι μηδενικό άθροισμα

Η προστασία της ιδιωτικότητας μέσου σχεδιασμού επιδιώκει την εξυπηρέτηση όλων των νόμιμων συμφερόντων και των στόχων ενός οργανισμού με θετικό «win-win»τρόπο. [24] Δηλαδή, χωρίς να γίνονται περιττοί συμβιβασμοί, προστατεύοντας περισσότερο ή μόνο την ιδιωτικότητα έναντι άλλων νόμιμων στόχων, όπως λ.χ. της ασφάλειας, αλλά στοχεύοντας να ικανοποιούνται όλοι οι νόμιμοι στόχοι, τονίζοντας, έτσι ότι είναι δυνατό και πολύ πιο επιθυμητό να αναζητούνται νέες λύσεις που να επιτρέπουν την πλήρη λειτουργικότητα, αποτελεσματικότητα και αποδοτικότητα των συστημάτων.[25]

1.2.5 Ασφάλεια από άκρο σε άκρο- Πλήρης προστασία κύκλου ζωής

Η Προστασία της ιδιωτικότητας από τον σχεδιασμό είναι ενσωματωμένη στο σύστημα κατά το αρχικό στάδιο, από τη συλλογή έως και την οριστική διαγραφή των δεδομένων προσωπικού χαρακτήρα, και επεκτείνεται καθ' όλη τη διάρκεια του κύκλου ζωής τους[26]. Δεν πρέπει να υφίστανται κενά στην προστασία, διότι μόνο έτσι δύναται να διασφαλιστεί η «αρχή της ασφάλειας». Προκειμένου να προστατευθούν τα δεδομένα σε όλα τα στάδια της επεξεργασίας τους, πρέπει να

[21]Cavoukian, 2010, p. 250
[22]AEPD, 2019, p.8
[23]Cavoukian, 2011,pp.1-2
[24] Ο.π.
[25]AEPD, 2019, p.8
[26]Ιγγλεζάκης,2013, σελ.76 επ.

εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένων, μεταξύ άλλων, των τεχνικών ψευδωνυμοποίησης ή ανωνυμοποίησης, κρυπτογράφησης, μεθόδων και τεχνικών ασφαλούς καταστροφής, καταγραφής κ.λπ.[27] Επομένως, με αυτόν τον τρόπο και με αυτά τα μέσα το PbD επιτυγχάνει την ασφαλή διαχείριση του κύκλου ζωής των προσωπικών δεδομένων, από άκρο σε άκρο.

1.2.6 Ορατότητα και διαφάνεια

Το PbD στοχεύει να διαβεβαιώσει σε όλα τα ενδιαφερόμενα μέρη ότι η επεξεργασία των προσωπικών τους δεδομένων, η οποία συντελείται μέσω της τεχνολογίας και της επιχειρηματικής πρακτικής, λειτουργεί σύμφωνα με τους σκοπούς, τους στόχους και τις δηλωμένες λειτουργίες του οργανισμού.[28] Οι εν λόγω λειτουργίες και διαδικασίες επεξεργασίας πρέπει να είναι ορατές, προσβάσιμες και διαφανείς[29] προς τα υποκείμενα των δεδομένων.

1.2.7 Σεβασμός της ιδιωτικότητας των χρηστών – μέριμνα για διαμόρφωση με βάση τις ανάγκες του χρήστη

Τα έννομα συμφέροντα ενός οργανισμού αναφορικά με την επεξεργασία των δεδομένων που εκτελεί είναι καίριας σημασίας, αλλά εξίσου σημαντική είναι και η διασφάλιση των δικαιωμάτων και ελευθεριών των χρηστών, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία. Το PbD απαιτεί από τους σχεδιαστές και χειριστές των συστημάτων να θέτουν και να διατηρούν στο επίκεντρο τα συμφέροντα των υποκειμένων των δεδομένων, παρέχοντας μέτρα, όπως, ισχυρές πολιτικές απορρήτου (privacy policies), κατάλληλες ειδοποιήσεις απορρήτου (privacy notices), ορθή ενημέρωση και συγκατάθεση του υποκειμένου των δεδομένων, καθώς και φιλικές επιλογές προς τον χρήστη για την προστασία της ιδιωτικότητας του.[30] Ως εκ τούτου οποιοδήποτε μέτρο εγκρίνεται πρέπει να

[27]Cavoukian,2011,pp.1-2
[28]Cavoukian, 2010, σ. 250
[29]Ιγγλεζάκης,2013, σελ.76 επ.
[30]Ιγγλεζάκης,2013, σελ.76 επ.

επικεντρώνεται στη διασφάλιση της προστασίας της ιδιωτικότητας των υποκειμένων των δεδομένων. Αυτό περιλαμβάνει το σχεδιασμό διαδικασιών και εφαρμογών, με επίκεντρο τα ενδιαφέροντα του χρήστη και την πρόβλεψη των αναγκών του. Επιπλέον, ο χρήστης πρέπει να διαδραματίζει ενεργό ρόλο στη διαχείριση των δεδομένων του λ.χ. μέσω της ελεύθερης και ειδικής συναίνεσής του για τη συλλογή, χρήση και αποκάλυψη των προσωπικών του ελευθεριών, αλλά και στον έλεγχο του τι κάνουν οι άλλοι με αυτά, χωρίς όμως να τεκμαίρεται ότι η αδράνεια του συνεπάγεται και την ελαττωμένη προστασία του.[31] Έτσι, το PbD εστιάζει, μεταξύ άλλων, στη διαχείριση του κινδύνου και στην υπευθυνότητα για τη θέσπιση στρατηγικών που αποσκοπούν στην προστασία της ιδιωτικής ζωής σε όλο τον κύκλο ζωής ενός αντικειμένου είτε πρόκειται για σύστημα, προϊόν υλικού ή λογισμικού, είτε για υπηρεσία ή διαδικασία. Η αρχή του PbD αναφέρεται στη φιλοσοφία και στην πρακτική της ενσωμάτωσης της προστασίας της ιδιωτικότητας σε όλα τα στάδια του σχεδιασμού και της ανάπτυξης συστημάτων και υπηρεσιών. Επομένως, ο τελικός στόχος είναι να διασφαλιστεί ότι η προστασία δεδομένων είναι παρούσα από τα πρώτα στάδια επεξεργασίας και αποτελεί αναπόσπαστο μέρος της φύσης του εν λόγω προϊόντος ή υπηρεσίας. Άρα, το PbD είναι ένα σύνολο μεθόδων, διαδικασιών και πρακτικών που στοχεύουν στην προληπτική ενσωμάτωση της προστασίας δεδομένων στα επιχειρηματικά μοντέλα των οργανισμών, επεκτείνοντας τα συστήματα τεχνολογίας πληροφοριών που υποστηρίζουν την επεξεργασία δεδομένων.

[31] AEPD,2019,p.10

ΚΕΦΑΛΑΙΟ 2ο ΤΕΧΝΟΛΟΓΙΕΣ ΕΝΙΣΧΥΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ–PRRIVACY ENCHANCING TECHNOLOGIES – PETs

2.1 Έννοια των PETs

Κατά τη δεκαετία του '90 είχε ξεκινήσει μια συζήτηση αναφορικά με την ανάγκη εισαγωγής και εφαρμογής Τεχνολογιών Πληροφορικής και Επικοινωνιών (εφεξής ΤΠΕ) με σκοπό την προστασία της ιδιωτικότητας. Οι εν λόγω ΤΠΕ προσδιορίστηκαν ως Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies ή -PETs), και αποτελούσαν αρχικά τεχνικές και οργανωτικές έννοιες και εργαλεία, που στόχευαν στην προστασία της προσωπικής ταυτότητας και της ιδιωτικότητας στα σύγχρονα πληροφοριακά και επικοινωνιακά συστήματα, που υποστηρίζουν υποδομές και υπηρεσίες.[32] Αρκετοί συγγραφείς χαρακτήριζαν τις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας ως μια γενική κατηγορία, η οποία περιλαμβάνει όλες τις τεχνολογίες που θα ήταν δυνατόν να επιτρέψουν στα άτομα να ελέγχουν τα όρια των αλληλεπιδράσεων τους με άλλους.[33]

Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας δεν έχουν ένα καθολικά συμφωνημένο και αποδεκτό ορισμό, παρά την ευρεία χρήση του όρου. Ωστόσο, είναι αξιοσημείωτο ότι οι υπάρχοντες ορισμοί χαρακτηρίζονται από ορισμένες κοινές αρχές, όπως ότι οι τεχνολογίες πρέπει να περιορίζουν ή να εξαλείφουν τον κίνδυνο παραβίασης των αρχών της ιδιωτικότητας και της νομοθεσίας για την προστασία της ιδιωτικής ζωής, να ελαχιστοποιούν τον όγκο των προσωπικών δεδομένων που κατέχει κάποιος για τα άτομα και, τέλος, να παρέχουν στα άτομα ανά πάσα στιγμή τον έλεγχο των πληροφοριών που τηρούνται και που τα αφορούν.[34] Επομένως, οι εν λόγω τεχνολογίες ενσωματώνουν τόσο τις θεμελιώδεις

[32] Μήτρου, 2013, σ.15
[33] Burkert, 1997, p.125.
[34] London Economics, 2010, p.7

αρχές προστασίας των δεδομένων, όσο και την ενσωμάτωση της απαίτησης για σεβασμό της ιδιωτικότητας κατά τον σχεδιασμό των τεχνολογιών, αφενός ελαχιστοποιώντας τη χρήση των προσωπικών δεδομένων, αφετέρου μεγιστοποιώντας την ασφάλεια των δεδομένων των χρηστών.[35]

Εν προκειμένω, ως Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας θα μπορούσε να οριστεί ένα ολοκληρωμένο σύστημα μέτρων ΤΠΕ, που σκοπός του είναι η προστασία της ιδιωτικότητας, εξαλείφοντας ή περιορίζοντας τη μη αναγκαία συλλογή, τήρηση, αποκάλυψη και διαμοιρασμό των προσωπικών δεδομένων, συχνά με τη παροχή εργαλείων που αποβλέπουν στην αύξηση του ελέγχου του ατόμου στα προσωπικά του στοιχεία, δίχως, όμως να απομειώνεται η λειτουργικότητα των πληροφοριακών συστημάτων. [36] Επομένως, οι εν λόγω Τεχνολογίες δύναται είτε να υφίστανται υπό τη μορφή εργαλείων, απαιτώντας, έτσι, μια θετική ενέργεια από τους χρήστες, οι οποίοι με τη σειρά τους πρέπει να προβούν σε δαπάνες αγοράς και εγκατάστασης αυτών στον προσωπικό τους ηλεκτρονικό υπολογιστή, είτε είναι ενσωματωμένες στο ίδιο το σύστημα. [37] Σύμφωνα με έναν άλλο ορισμό, του Οργανισμού της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο - ENISA[38] ως PETs ορίζονται οι «λύσεις λογισμικού και υλικού, δηλαδή συστήματα που περιλαμβάνουν τεχνικές διαδικασίες, μεθόδους ή γνώσεις, που αποσκοπούν στην επίτευξη συγκεκριμένων λειτουργιών προστασίας της ιδιωτικής ζωής ή προστασίας των δεδομένων ενός υποκειμένου ή μιας ομάδας φυσικών προσώπων».[39] Στο σημείο, όμως, αυτό πρέπει να τονιστεί ότι τα PETs δεν πρέπει να λογίζονται μόνο ως κομμάτια λογισμικού ή υλικού που δύναται να αναμειχθούν και να συνδυαστούν, αλλά ως ολοκληρωμένα συστήματα προστασίας της ιδιωτικής ζωής.[40]

Ωστόσο, η εφαρμογή της έννοιας των PETs σε συγκεκριμένες τεχνολογίες δεν είναι πάντα μια απλή διαδικασία. Συγκεκριμένα, είναι καίριο να σημειωθεί ότι

[35]Nietoet.al., 2019, p.11

[36]Μήτρου, 2013, σ.15
[37]Ο.π
[38]https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32019R0881&from=PT
[39]Information Commissioner's office, 2023,p.5
[40]London Economics, 2010, p.7

ανεξαρτήτως του γεγονότος ότι αρκετές τεχνολογίες ασφαλείας πληροφοριών εφαρμόζονται και για τη παροχή ιδιωτικότητας (π.χ. μηχανισμοί κρυπτογράφησης), δεν ανήκουν όλα τα μέτρα ασφαλείας στην έννοια των PETs. Όπως προκύπτει και από την έκθεση του 1995 του Επιτρόπου Δεδομένων αναφορικά με τα PETs η ασφάλεια των πληροφοριών είναι σημαντική και αναγκαία, αλλά οι τεχνολογίες ασφάλειας των πληροφοριών που χρησιμοποιούνται δεν είναι πάντα «αληθινές» PETs, καθώς μπορούν να χρησιμοποιηθούν με τρόπους και μέσα που στην πραγματικότητα παραβιάζουν αντί να προστατεύουν την ιδιωτική ζωή[41], όπως συμβαίνει με αρκετούς ελέγχους ασφαλείας που χρησιμοποιούν εφαρμογές που εισβάλουν στην ιδιωτικότητα (π.χ. εργαλεία παρακολούθησης).[42]

2.2 Βασικά χαρακτηριστικά και ταξινόμηση των PETs σε κατηγορίες

Από τα παραπάνω διαφαίνεται η σύνθετη έννοια των PETs, η οποία σε συνδυασμό με τη μη ύπαρξη ενός κοινά αποδεκτού ορισμού και τη μεγάλη ποικιλία τους, γίνεται αντιληπτό το μεγάλο μέγεθος της πρόκλησης που δημιουργείται. Από το πρώτο στάδιο της εμφάνισης των PETs μέχρι και σήμερα έχουν πραγματοποιηθεί πληθώρα συζητήσεων αναφορικά με τα ποια πρέπει να είναι τα χαρακτηριστικά τους. Ο Goldeberg απαριθμεί μια σειρά από γενικές ιδιότητες των τεχνολογιών που είναι απαραίτητες για να μπορέσουν οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας να είναι χρήσιμες, όπως είναι η ευχρηστία, η ικανότητα ανάπτυξης, η αποτελεσματικότητα και η ευρωστία. Ειδικότερα, αναφορικά με την πρώτη ιδιότητα, οι χρήστες πρέπει να είναι σε θέση να χρησιμοποιήσουν ορθά μια Τεχνολογία Ενίσχυσης της Ιδιωτικότητας και να έχουν την επιθυμία να τη χρησιμοποιήσουν, με δεδομένο το κόστος, αλλά και τις δυσκολίες που ενδέχεται να αντιμετωπίσουν. Αναφορικά με την ικανότητα ανάπτυξης, οι καθημερινοί χρήστες πρέπει να είναι σε θέση να αποκτήσουν και να επωφεληθούν από μια Τεχνολογία Ενίσχυσης της Ιδιωτικότητας. Αυτό σημαίνει ότι πρέπει να είναι συμβατή, μεταξύ άλλων, με το προτιμώμενο λειτουργικό σύστημα και το

[41] London Economics,2020,p.7
[42]Μήτρου,Καρυδά,2012, σ.3

πρόγραμμα περιήγησης στο διαδίκτυο. Ιδανικά, η Τεχνολογία Ενίσχυσης της Ιδιωτικότητας θα πρέπει να είναι ενσωματωμένη, ώστε ο χρήστης να μην χρειάζεται να βρει και να εγκαταστήσει ξεχωριστά πακέτα λογισμικού. Προκειμένου να πληρείται το στοιχείο της αποτελεσματικότητας, η τεχνολογία πρέπει φυσικά να λειτουργεί και να προσφέρει στον χρήστη το όφελος που υπόσχεται. Τέλος, με την ευρωστία νοείται ότι το σύστημα πρέπει να διατηρεί όσο το δυνατόν μεγαλύτερη προστασία στους χρήστες, λ.χ. από ιούς και από επιθέσεις phishing.[43]

Η ραγδαία αύξηση του αριθμού τους οδήγησε στη προσπάθεια ταξινόμησης τους. Είναι γεγονός, όμως, ότι παρά τη πληθώρα ταξινομήσεων, καμία δεν έχει τύχει κοινής αποδοχής. Οι περισσότερες Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας είναι σύνθετες τεχνολογίες που χρησιμοποιούν τεχνικές ασφαλείας, όπως η κρυπτογράφηση και οι μηχανισμοί ελέγχου πρόσβασης, σε συνδυασμό με άλλους μηχανισμούς, στοχεύοντας στη βελτίωση της προστασίας της ιδιωτικότητας.[44] Επιπροσθέτως, οι PETs προσφέρουν στους χρήστες τη δυνατότητα να ασκούν έλεγχο σχετικά με τη κοινοποίηση και μετάδοση των δεδομένων τους, επιτρέποντας τους, να ελέγχουν ποια προσωπικά δεδομένα επεξεργάζονται, με ποιο τρόπο και από ποιόν (π.χ. έλεγχοι ιδιωτικότητας, εργαλεία ελαχιστοποίησης δεδομένων και αρχεία καταγραφής).[45] Δύναται, επίσης, να επιτρέπουν στους χρήστες να αποκρύπτουν την πραγματική τους ταυτότητα και να πλοηγούνται στο Διαδίκτυο «ανώνυμα» ή με «ψευδώνυμο».[46] Άλλες PETs περιλαμβάνουν φίλτρα και blockers, διαγραφείς ψηφιακών ιχνών (track and evidence erasers), μηχανισμούς συναίνεσης, συστήματα διαχείρισης ψηφιακής ταυτότητας, οι επονομαζόμενοι privacy proxies (μεσολαβητές ιδιωτικότητας).[47]

Παρακάτω, θα αναλυθούν οι εφαρμοζόμενες τεχνικές της κρυπτογράφησης, ψευδωνυμοποίησης, ανωνυμοποίησης, και tokenazitation, που χρησιμοποιούνται

[43]Goldeberg, 2007, p.11
[44]Μήτρου, Καρυδά, 2012, σ.3
[45]Ο.π
[46]Ο.π
[47]Μήτρου,2012, σ. 16

στον τομέα της ιδιωτικότητας και προσφέρουν λύσεις στην προστασία των προσωπικών δεδομένων.

2.2.1 Κρυπτογράφηση

Ο ΓΚΠΔ δεν περιλαμβάνει έναν ακριβή ορισμό της κρυπτογράφησης, ωστόσο ο όρος αυτός θα μπορούσε να περιγραφεί ως η εφαρμογή μια διαδικασίας μετασχηματισμού ενός συνόλου προσωπικών δεδομένων σε μια ακατάληπτη μορφή, με βάση κάποιον αλγόριθμο, αλλά και με τη χρήση «κλειδιών κρυπτογράφησης», ώστε η αναγνώριση τους να καθίσταται αδύνατη για τον καθένα, αλλά να αναγνωρίζεται μόνο από τον νόμιμο ιδιοκτήτη των κλειδιών κρυπτογράφησης.[48] Έτσι, μόνο όποιος γνωρίζει το μυστικό κλειδί έχει τη δυνατότητα να ανακτήσει τα αρχικά δεδομένα από τα κρυπτογραφημένα. Επομένως, η διαδικασία είναι αντιστρεπτή, γίνεται μια αποκρυπτογράφηση, η οποία είναι εφικτή μόνο από εξουσιοδοτημένους χρήστες που γνωρίζουν το κλειδί αποκρυπτογράφησης. Η ασφάλεια αυτής της τεχνικής βασίζεται στη «μυστικότητα του κλειδιού».[49] Άρα, είναι υψίστης σημασίας η απαίτηση για διαχείριση και προστασία των «μυστικών κλειδιών», αφού η απώλεια τους ισοδυναμεί με απώλεια προσωπικών δεδομένων.[50] Ως τεχνική, η κρυπτογράφηση, θεωρείται αρκετά ασφαλής, ειδικά όταν γίνεται χρήση εξελιγμένων μηχανισμών κρυπτογράφησης, αλλά δε θα μπορούσε να θεωρηθεί και αρκετά εύχρηστη, δεδομένου ότι η επεξεργασία των κρυπτογραφημένων δεδομένων απαιτεί πρώτα την αποκρυπτογράφηση τους, μια διαδικασία που χρειάζεται τόσο υπολογιστικούς πόρους, όσο και επιπλέον χρόνο. Επομένως, μια πρόκληση που έχει να αντιμετωπίσει η εν λόγω τεχνική είναι η εξισορρόπηση ανάμεσα στην ασφάλεια των προσωπικών δεδομένων και στην χρηστικότητα του τεχνικού μέτρου ασφαλείας.[51]

[48] Λουκάς,2017,σ. 47
[49]Τιντζογλίδου, 2021, σ.88
[50] Λουκάς,2017, σ.48
[51]Ο.π.

2.2.2 Ψευδωνυμοποίηση

Ο ΓΚΠΔ ορίζει επαρκώς την τεχνική της ψευδωνυμοποίησης, έτσι σύμφωνα με το άρθρο 4 παρ. 5 του Κανονισμού «*Ψευδωνυμοποίηση είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*». Η Ψευδωνυμοποίηση ως τεχνικό μέτρο αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιον τρόπο, όπως, μέσω της χρήσης τυχαίων χαρακτήρων, έτσι ώστε, να απαιτούνται πρόσθετες πληροφορίες, προκειμένου να αναγνωριστεί εκ νέου το υποκείμενο των δεδομένων. Αποτελεί μια αναστρέψιμη διαδικασία, δηλαδή οδηγεί στην ταυτοποίηση του υποκειμένου, η οποία είναι εφικτή μέσω της χρήσης ενός ενδιάμεσου πίνακα αντιστοιχίας των κωδικών ή άλλων αναγνωριστικών στοιχείων που έχουν χρησιμοποιηθεί και, μπορούν να οδηγήσουν επαγωγικά στα πραγματικά στοιχεία των ατόμων, όπως είναι το ονοματεπώνυμο ή διεύθυνσή τους.

Ως τεχνική είναι πολύ πιο εύχρηστη από την τεχνική της κρυπτογράφησης, καθώς τα ψευδωνυμοποιημένα δεδομένα δεν μπορούν να αποδοθούν σε κάποιο υποκείμενο, ενώ, συγχρόνως η επεξεργασία τους συνιστά μια πιο εύκολη διαδικασία. Ωστόσο, ελλοχεύει ο κίνδυνος, σε περίπτωση απόκτησης του μηχανισμού ψευδωνυμοποίησης από ένα τρίτο άτομο ή σε περίπτωση σύνδεσης με άλλο τρόπο του ψευδωνυμοποιημένου συνόλου δεδομένων με τα υποκείμενα, να παραβιαστούν τα δεδομένα και εν τέλει να ταυτοποιηθεί το υποκείμενο των δεδομένων.[52] Απόδειξη αποτελεί μια μελέτη, σύμφωνα με την οποία ένα μεγάλο ποσοστό Αμερικανών πολιτών, το οποίο κυμαίνεται στη κλίμακα του 87% μπορεί να αναγνωριστεί με μοναδικό τρόπο, απλώς με τον συνδυασμό τριών απλών και

[52] Ο.π.

«αθώων» δημογραφικών στοιχείων, όπως η ημερομηνία γέννησης, το φύλο και ο ταχυδρομικός κώδικας. [53] Για αυτόν τον λόγο, οι υπεύθυνοι επεξεργασίας οφείλουν να μεριμνούν και να λαμβάνουν κατάλληλα τεχνικά μέτρα αποτροπής της εύκολης αναστροφής της διαδικασίας, όπως προβλέπει και το γράμμα της διάταξης του ΓΚΠΔ, η οποία θέτει ως απαίτηση οι «*συμπληρωματικές πληροφορίες*» να διατηρούνται σε ξεχωριστή τοποθεσία και να υπόκεινται σε κατάλληλα τεχνικά και οργανωτικά μέτρα. Επομένως, για να αποτραπεί μια εκ νέου αναγνώριση των υποκειμένων, συνιστάται π.χ. η χρήση μεθόδων κρυπτογραφίας ή αντικατάσταση χρήσιμης πληροφορίας με άχρηστη πληροφορία, όπως μάρκες (tokens), κ.λπ.[54]

2.2.3 Ανωνυμοποίηση

Η Ανωνυμοποίηση αρκετά συχνά συγχέεται με την Ψευδωνυμοποίηση στο πεδίο της προστασίας και της ασφάλειας των Δεδομένων, ωστόσο, πρόκειται για δύο διαφορετικές τεχνικές, ειδικά στο πλαίσιο του ΓΚΠΔ, όπου τα «ανωνυμοποιημένα» και τα «ψευδωνυμοποιημένα» δεδομένα αντιμετωπίζονται ως δύο εντελώς διαφορετικές κατηγορίες. Η Ανωνυμοποίηση, σε αντίθεση με την Ψευδωνυμοποίηση, αποτελεί μια διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, ώστε να μην είναι πλέον εφικτό αυτά τα δεδομένα που έχουν υποστεί ανωνυμοποίηση, να συσχετιστούν και να συνδεθούν με το υποκείμενο των δεδομένων. [55] Επομένως, το υποκείμενο δεν μπορεί να ταυτιστεί μέσα σε ένα σύνολο υποκειμένων, το λεγόμενο σύνολο ανωνυμίας, το οποίο είναι το σύνολο πιθανών υποκειμένων.[56]Αναλυτικότερα, τα δεδομένα αποκτούν μια ανώνυμη μορφή, μέσω της χρήσης κατάλληλων τεχνικών και λογισμικών εργαλείων, και έτσι δεν μπορούν να συσχετιστούν με κάποιο άλλο άτομο. Η ανωνυμοποίηση υλοποιείται, μεταξύ άλλων, με τη τεχνική της

[53]Sweeney, 2000,pp.1-34
[54]Κανέλλος,2020,σ. 43
[55]Λουκάς, 2017,σ.47
[56]Pfitzmann and Hansen, 2010, p.9

γενίκευσης γνωρισμάτων των υποκειμένων (generalization), η οποία αποσκοπεί στην απόκρυψη της ταυτότητας των ατόμων μέσω της ένταξης τους σε μια μεγαλύτερη ομάδα με παρόμοια χαρακτηριστικά. Π.χ. μια έννοια ειδικού επαγγέλματος, όπως ο «πνευμονολόγος» ή ο «καρδιολόγος», μπορεί να αντικατασταθεί από μια έννοια γένους, όπως «ιατρικό επάγγελμα». Ένα ακόμη παράδειγμα γενίκευσης μπορεί να εφαρμοστεί στην παρουσίαση προσωπικών δεδομένων, όπως η ηλικία. Έτσι, αντί για την ακριβή δήλωση της ηλικίας ενός ατόμου, χρησιμοποιείται ένα εύρος ηλικιών, όπως «20-30 ετών». Έτσι, αποφεύγεται το υποκείμενο να ταυτοποιηθεί μόνο χάρη σε αυτά τα αναγνωριστικά στοιχεία. Η διαδικασία της ανωνυμοποίησης απαιτεί μεγάλη προσοχή από τον υπεύθυνο επεξεργασίας, καθώς είναι πιθανό, να μην μπορεί να ισχυριστεί με βεβαιότητα ότι έχει επιτευχθεί ανωνυμοποίηση των δεδομένων, ακόμη και με τη χρήση τεχνικών ανωνυμοποίησης. Και σε αυτό το σημείο είναι που ο υπεύθυνος επεξεργασίας μπορεί να πιστεύει λανθασμένα ότι αν δεν είναι «καταφανές» σε ποιο υποκείμενο αναφέρονται τα δεδομένα, τότε είναι και ανώνυμα. Όμως, το ορθό είναι να θεωρείται πως ακόμα και αν δεν είναι προφανής η ταυτότητα του υποκειμένου στο οποίο αναφέρονται τα δεδομένα, πρέπει, προτού χαρακτηριστούν ως ανώνυμα, να ελεγχθεί ενδελεχώς, αν πράγματι έχει «εκμηδενιστεί» η δυνατότητα ανακάλυψης της ταυτότητάς του υποκειμένου.[57]Είναι γεγονός ότι, συχνά τα δεδομένα αποτελούν μεν ασύνδετες πληροφορίες, ωστόσο, είναι δυνατόν, με τη βοήθεια τεχνικών συνδυαστικής ανάλυσης και συγκερασμού πληροφοριών που προσφέρουν οι σύγχρονες τεχνολογίες να οδηγηθεί κάποιος στην επαναταυτοποίηση ενός ατόμου. [58] Επομένως, η μέθοδος της ανωνυμοποίησης φαίνεται να παρουσιάζει ορισμένες δυσκολίες και να μην εξασφαλίζει πάντα την πολυπόθητη ιδιωτικότητα. [59]

Επιπροσθέτως, είναι σημαντικό να τονιστεί ότι, σύμφωνα με την αιτιολογική σκέψη 26 του ΓΚΠΔ, «*Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο*

[57]Τιντζογλίδου, 2022, σ.91
[58] Μήτρου,2024,σ.29
[59] Κανελλοπούλου –Μπότη,2020, σ.107

φυσικό πρόσωπο». Αντιθέτως, *«Οι αρχές της προστασίας δεδομένων δεν θα πρέπει συνεπώς να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί».* Επομένως, ο Κανονισμός δεν αφορά την επεξεργασία τέτοιων ανώνυμων πληροφοριών, σε αντίθεση με τα ψευδωνυμοποιημένα δεδομένα, τα οποία παραμένουν προσωπικά δεδομένα και ως τέτοια υπόκεινται στις διατάξεις του ΓΚΠΔ. Το γεγονός ότι, ως τεχνικό μέτρο η ανωνυμοποίηση δεν εμπίπτει στο νομοθετικό καθεστώς που προδιαγράφει ο ΓΚΠΔ, ενδέχεται να θεωρηθεί ως μια στρατηγική επιλογή ενός υπεύθυνου επεξεργασίας, ο οποίος δε θα είναι υποχρεωμένος να υπακούει στο σύνολο των διατάξεων του ΓΚΠΔ. Η ανωνυμοποίηση, μπορεί να είναι μια δελεαστική επιλογή σε ορισμένες περιπτώσεις, ωστόσο, δεν αποτελεί μια τυπική επιλογή για τους υπεύθυνους επεξεργασίας. Δεδομένου ότι, αποτελεί μια μη αναστρέψιμη διαδικασία, η οποία ακυρώνει την δυνατότητα αναγνώρισης των υποκειμένων των δεδομένων. Απόρροια της οποίας είναι, ενδεχομένως, η υποβάθμιση της χρηστικότητας και εν τέλει της χρησιμότητας των ανωνυμοποιημένων δεδομένων.[60]

2.2.4 Tokenisation

Αποτελεί ένα τεχνικό μέτρο ασφαλείας, το οποίο αντικαθιστά ευαίσθητα προσωπικά δεδομένα, όπως ο αριθμός φορολογικού μητρώου (ΑΦΜ), ιατρικά δεδομένα ασθενών ή αριθμούς πιστωτικών καρτών, διαβατηρίων και ταυτοτήτων με τυχαία σύμβολα ή tokens (μάρκες), τα οποία δεν έχουν καμία μαθηματική σχέση ή άλλη συσχέτιση με τα αρχικά δεδομένα που περιείχαν πρωτογενείς πληροφορίες. Τα πραγματικά δεδομένα αποθηκεύονται σε μια χωριστή και προστατευμένη βάση δεδομένων (token vault), που είναι ένα αυστηρά ελεγχόμενο και με διαβαθμισμένη πρόσβαση φυλασσόμενο σύστημα. Σε περίπτωση, δε, απώλειας ή κλοπής των tokens, δεν υφίσταται κίνδυνος αποκάλυψης των αρχικών

[60] Λουκάς,2017,σ.48

ευαίσθητων πληροφοριών, καθώς δεν είναι δυνατόν να ανασυντεθούν από την αντίστροφη διαδικασία, δηλαδή από τα tokens.[61]

2.3 Προκλήσεις στη διάδοση των τεχνολογιών ενίσχυσης της Ιδιωτικότητας

Η ανάπτυξη και υιοθέτηση των PETs, εξαιρουμένης της κρυπτογράφησης, η οποία γνώρισε ευρεία διάδοση και αποδοχή, υπήρξε κατώτερη των προσδοκιών των εμπνευστών τους, καθώς, τελικά δεν κατάφεραν να εξελιχθούν σε βασικό συστατικό του σχεδιασμού συστημάτων.[62] Η μη διάδοση των PETs και η μη επέκταση τους στο βαθμό που πίστευαν και ήλπιζαν οι εμπνευστές τους βασίζεται σε πολλούς και διαφορετικούς παράγοντες.

Αρχικά, η ζήτηση των PETs εκ μέρους των χρηστών δεν ήταν ανάλογη των επιφυλάξεων και των ανησυχιών που διατύπωναν σχετικά με την προστασία των προσωπικών τους δεδομένων και με τους κινδύνους για την πληροφοριακή ιδιωτικότητα[63]. Αυτό ενδέχεται να οφείλεται στην ελλιπή πληροφόρηση, στην έλλειψη προηγούμενης εμπειρίας ή στην έλλειψη ικανοποιητικού και επαρκούς επιπέδου γνώσεων επί της λειτουργίας των εν λόγω Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας.[64] Ακολούθως, προϋπόθεση για την ενεργητική επιλογή χρήσης των τεχνολογιών αυτών από τα υποκείμενα των δεδομένων, δεν είναι μόνο η πληροφόρηση και οι γνώσεις τους για τα PETs, ούτε η συνειδητοποίηση της ύπαρξης κινδύνων για τα προσωπικά τους δεδομένα, αλλά και η εκτίμηση ότι οι κίνδυνοι αυτοί μπορούν να αντιμετωπιστούν κατά τρόπο αποτελεσματικό.[65] Απόδειξη σε αυτό αποτελεί μια έρευνα, η οποία επικεντρώθηκε στην ενσωμάτωση της αρχής PbD στην ηλεκτρονική δημόσια διοίκηση. Μεταξύ των πορισμάτων της ήταν και ο σκεπτικισμός των συμμετεχόντων σχετικά με την αποτελεσματικότητα των PETs, εξαιτίας της πολυπλοκότητας τους. Επομένως, αν και τα PETs έχουν σχεδιαστεί για την προστασία της ιδιωτικής ζωής των χρηστών,

[61] Κανέλλος,2020,σ.45
[62] Γιαννόπουλος, Μήτρου, Τσόλιας, 2021, σ.275
[63] Ο.π
[64] Μήτρου, Καρυδά, 2012, σελ. 4
[65] Μήτρου, 2012,σ.17

η χρήση τους δεν οδηγεί πάντα σε αυξημένη εμπιστοσύνη ή αποδοχή μεταξύ των χρηστών. [66] Πρέπει να τονιστεί ότι συχνά η πραγματική εφαρμογή των PETs αποτελεί μια αρκετά απλή διαδικασία, αλλά, πράγματι, η πολυπλοκότητα του όρου δυσκολεύει τους ενδιαφερόμενους χρήστες, να κατανοήσουν την χρησιμότητά τους και εντέλει να τις εφαρμόσουν. [67] Ωστόσο, ορισμένες PETs πράγματι, δεν πληρούν το στοιχείο της αποτελεσματικότητας, καθώς παραμένουν ανεπαρκώς ανεπτυγμένες, εξακολουθούν να είναι αδύναμες στο στάδιο της εφαρμογής, και συχνά εφαρμόζονται με αναποτελεσματικούς τρόπους.[68]

Επιπλέον, η προστασία της ιδιωτικότητας αποτελεί παράγοντα πρόσθετου κόστους, σε αντίθεση με την επεξεργασία προσωπικών δεδομένων, η οποία συνιστά μια δραστηριότητα που επιφέρει ολοένα και περισσότερα κέρδη. [69] Επομένως, το επιπλέον κόστος που ενέχουν οι ως άνω τεχνολογίες, σε συνδυασμό με την έλλειψη νομικής υποχρέωσης, η οποία θα επιβάλει την υιοθέτηση τέτοιων τεχνολογιών, έχουν ως αποτέλεσμα τον περιορισμό των επενδύσεων στον τομέα Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας.[70]Έτσι, παρά το γεγονός ότι οι κίνδυνοι που συνδέονται με τη χρήση προσωπικών δεδομένων σε ηλεκτρονική μορφή είναι σοβαροί, παράλληλα με την ολοένα και αυξανόμενη ανησυχία των υποκειμένων των δεδομένων αναφορικά με την προστασία των προσωπικών τους δεδομένων, θα έπρεπε το ποσοστό διάδοσης και υιοθέτησης των PETs να είναι θεαματικά υψηλό, ωστόσο, κάτι τέτοιο φαίνεται να μην ισχύει. Όπως έχουν δείξει και πορίσματα μελετών, μπροστά στο δίπολο προστασία της ιδιωτικότητας και άλλες ωφέλειες, η ζυγαριά τείνει να κλείνει προς το δεύτερο.[71]

2.4 Η σχέση των PETsμε το PbD

Η περιορισμένη διάδοση των PETs μαζί με την αυξανόμενη χρήση των ΤΠΕ ανέδειξε την ανάγκη για έναν ευρύτερο σχεδιασμό της προστασίας. Η αρχική

[66]Kooletal., 2011, p. 1-90
[67]Μήτρου, Καρυδά, 2012, σ. 3
[68]Ο.π, σ.4
[69] Μήτρου 2012, σ.17
[70]Γιαννόπουλος, Μήτρου, Τσόλιας, 2021, σ.275

[71]Acquisti,2010, pp.36

συζήτηση γύρω από τα ζητήματα που ανακύπτουν με τις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας εξελίχθηκε σε συζήτηση γύρω από την ιδιωτικότητα εκ σχεδίου και δια σχεδιασμό .[72] Επιπροσθέτως, τόσο τα PETs, όσο η έννοια του PbD δεν έχουν έναν κοινά αποδεκτό ορισμό. Συχνά, αυτή η έλλειψη τείνει να δημιουργεί την λανθασμένη εντύπωση ότι οι εν λόγω έννοιες ταυτίζονται. Ωστόσο, οι PETs είναι εφαρμογές ή εργαλεία, τα οποία αποσκοπούν να καλύψουν μια πτυχή της ιδιωτικότητας, ενισχύοντας την απόδειξη μιας προσέγγισης «προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού», μέσω της τήρησης της αρχής της ελαχιστοποίησης των δεδομένων, παρέχοντας κατάλληλο επίπεδο ασφάλειας, εφαρμόζοντας ισχυρές λύσεις ανωνυμοποίησης ή ψευδωνυμοποίησης και ελαχιστοποιώντας τον κίνδυνο που προκύπτει από παραβιάσεις προσωπικών δεδομένων, καθιστώντας τα προσωπικά δεδομένα και τις προσωπικές πληροφορίες ακατάληπτα σε οποιονδήποτε δεν έχει δικαίωμα πρόσβασης σε αυτά. Από την άλλη, το PbD υπερβαίνει τη θετική συμβολή της τεχνολογίας, επί της οποίας βασίζεται η προσέγγιση των PETs, συνιστώντας, έτσι, μια ολιστική προσέγγιση στο σχεδιασμό οποιασδήποτε τεχνολογίας, η οποία περικλείει τη ιδιωτικότητα τόσο στην αρχιτεκτονική, όσο και στις προδιαγραφές της, χωρίς να περιορίζεται στη τεχνολογική υποστήριξη μια εφαρμογής.[73]

[72]Μήτρου,2013, σ. 17
[73]Rubinstein, 2012, p.1409

Κεφάλαιο 3ο ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ (PRIVACY BY DESIGN) ΣΤΟΝ ΓΕΝΙΚΟ ΚΑΝΟΝΙΣΜΟ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Σε έναν κόσμο που ολοένα και ψηφιοποιείται συνδυαστικά και με τις ραγδαίες τεχνολογικές εξελίξεις η ρυθμιστική διαδικασία των νομικών κανόνων αναφορικά με τη προστασία των δικαιωμάτων στη πληροφοριακή ιδιωτικότητα αποτελεί ένα απαιτητικό και γεμάτο προκλήσεις εγχείρημα.[74] Από τις 18 Μαΐου 2018 εφαρμόζεται άμεσα ο ΓΚΠΔ σε κάθε κράτος μέλος της ΕΕ, καταργώντας την Οδηγία 95/46/ΕΚ *«για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»*. Μπορεί η εν λόγω Οδηγία να καταργήθηκε από τον ΓΚΠΔ, εμφανίζει, ωστόσο, ορισμένα στοιχεία της αρχής της ιδιωτικής ζωής από τον σχεδιασμό. Πιο συγκεκριμένα, η αιτιολογική σκέψη 46 της Οδηγίας σημειώνει ότι πρέπει να εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δικαιωμάτων και ελευθεριών των ατόμων, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία.[75]Σύμφωνα με το άρθρο 17 της οδηγίας 95/46/ΕΚ ορίζεται ότι οι υπεύθυνοι επεξεργασίας και κατά περίπτωση οι εκτελούντες την επεξεργασία έχουν τη νομική και όχι απλώς τη δεοντολογική υποχρέωση να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των προσωπικών δεδομένων. Η εν λόγω υποχρέωση εξειδικεύεται υπό μια έννοια από τον νομοθέτη, καθώς πρέπει να εξασφαλίζεται ανάλογο επίπεδο ασφάλειας των προσωπικών δεδομένων ως προς τους κινδύνους που συνεπάγεται

[74]Μήτρου, 2013, σ.14

[75] «*η προστασία των δικαιωμάτων και ελευθεριών των προσώπων στα οποία αναφέρονται τα δεδομένα έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα απαιτεί τη λήψη κατάλληλων τεχνικών μέτρων και οργάνωση κατά τη στιγμή τόσο του σχεδιασμού των τεχνικών επεξεργασίας όσο και της εκτέλεσης της επεξεργασίας, προκειμένου ιδίως να υπάρξουν εγγυήσεις για την ασφάλειά τους και να εμποδίζεται έτσι κάθε ανεπίτρεπτη επεξεργασία· ότι εναπόκειται στα κράτη μέλη να μεριμνούν για την τήρηση των μέτρων αυτών εκ μέρους των υπευθύνων της επεξεργασίας- ότι τα μέτρα αυτά πρέπει να εξασφαλίζουν ενδεδειγμένο επίπεδο ασφάλειας, λαμβάνοντας υπόψη την κατάσταση της τεχνικής και το κόστος της εφαρμογής τους έναντι των κινδύνων που εμφανίζουν οι επεξεργασίες και της φύσης των προς προστασία δεδομένων».*

τόσο η επεξεργασία των δεδομένων, όσο και η φύση αυτών που αποτελούν αντικείμενο της επεξεργασίας[76].

3.1 Το άρθρο 25 παρ.1 του ΓΚΠΔ

Ο ΓΚΠΔ με το άρθρο 25 υποχρεώνει τους υπεύθυνους επεξεργασίας, ανεξάρτητα από το μέγεθος και την πολυπλοκότητα της επεξεργασίας που συντελούν, να εφαρμόζουν τις νομικές υποχρεώσεις τους κατά τον σχεδιασμό των πράξεων επεξεργασίας.[77] Η πρακτική αυτή συνιστά μια πολύπλευρη και απαιτητική διαδικασία, η οποία περιλαμβάνει ένα πλήθος από τεχνικές και τεχνολογίες, οι οποίες προβλέπουν την εφαρμογή των αρχών προστασίας της ιδιωτικότητας σε πληροφοριακά συστήματα, λογισμικά, εφαρμογές και υπηρεσίες.[78] Επιπλέον, η προστασία των προσωπικών δεδομένων από τον σχεδιασμό αποτελεί μια έννοια που έχει χαρακτηριστεί ως η βέλτιστη νομοτεχνική πρακτική για την προστασία της ιδιωτικότητας των υποκειμένων των δεδομένων. Ο ΓΚΠΔ με τη νομοθετική πρόβλεψη του άρθρου 25 λαμβάνει υπόψη τις βαρύνουσες αλλαγές που επέφερε στην καθημερινότητα η επικρατούσα υιοθέτηση του διαδικτύου και γενικότερα ο ψηφιακός μετασχηματισμός[79]και καταγράφει τις απαραίτητες ρυθμίσεις, ώστε ο τρόπος εφαρμογής και επιβολής αυτής της νομικής υποχρέωσης από τους υπεύθυνους επεξεργασίας να αποτελέσει το βασικό στοιχείο ως προς την καταλληλότερη και αποτελεσματικότερη προστασία των δεδομένων των υποκειμένων.[80]

Για την καλύτερη κατανόηση και διερεύνηση των σχετικών απαιτήσεων και τεχνολογικών προσεγγίσεων είναι σκόπιμο να ακολουθήσει μια περαιτέρω ανάλυση, η οποία τείνει να αποκρυπτογραφήσει τη διάταξη του άρθρου 25 ΓΚΠΔ. Έτσι, το άρθρο 25, παρ. 1 του ΓΚΠΔ προβλέπει ότι: «*Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους*

[76]Μήτρου,2013, σ.18
[77]European Data Protection Supervisor, 5/2018,p. 4
[78]Λουκάς,2018, σελ.38 επ.
[79]LabadieandLegner,2020, p.2
[80]Λουκάς,2019, σελ.46-51

διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποκλειστικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. Εν προκειμένω, λαμβάνει υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία».

Με την καθιέρωση του ως άνω άρθρου η προστασία των δεδομένων από τον σχεδιασμό δεν συνιστά πλέον μια επιθυμία ή απλώς μια συνιστώμενη καλή πρακτική, αλλά αποτελεί μια νομική υποχρέωση, με την οποία οφείλουν να συμμορφώνονται όλοι όσοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσης.[81]Στη τεκμηρίωση της προστασίας δεδομένων από τον σχεδιασμό συνηγορεί και η αιτιολογική σκέψη 78 του ΓΚΠΔ, σύμφωνα με την οποία «*η προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα απαιτεί τη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε να διασφαλίζεται ότι τηρούνται οι απαιτήσεις του παρόντος κανονισμού. Προκειμένου να μπορεί να αποδείξει συμμόρφωση προς τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να θεσπίζει εσωτερικές πολιτικές και να εφαρμόζει μέτρα τα οποία ανταποκρίνονται ειδικότερα στις αρχές της προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού. Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα το*

[81]European Data Protection Supervisor, Opinion 5/2018, p.3

συντομότερο δυνατόν, τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφαλείας.

Με βάση την υποχρέωση του άρθρου 25 παρ. 1 του ΓΚΠΔ, η εφαρμογή της προστασίας των δεδομένων ήδη από τον σχεδιασμό εστιάζει μόνο στους υπευθύνους της επεξεργασίας, ωστόσο, είναι αξιοσημείωτο, το περιεχόμενο του εδαφίου δ' της αιτιολογικής σκέψης 78 του κανονισμού, το οποίο αναφέρει ότι «*Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων*».

Επομένως, η διάταξη του άρθρου 25 παρ. 1 δε θα πρέπει να περιορίζεται μόνο στους υπεύθυνους επεξεργασίας, αλλά θα πρέπει να περιλαμβάνει και τους εκτελούντες την επεξεργασία και τους παραγωγούς προϊόντων, υπηρεσιών και εφαρμογών, ώστε να ενθαρρύνονται να υπολογίζουν το δικαίωμα προστασίας των δεδομένων των υποκειμένων κατά τον σχεδιασμό των εν λόγω προϊόντων και υπηρεσιών τους. Άρα, αυτή η υποχρέωση μπορεί να μη περιλαμβάνεται στις ουσιαστικές διατάξεις του ΓΚΠΔ, ωστόσο, το κενό αυτό που δημιουργείται και ευλόγως προκαλεί ερμηνευτική δυσχέρεια, καλύπτεται, κατά ένα βαθμό, από την ως άνω αιτιολογική σκέψη.[82]

[82]Κατευθυντήριες γραμμές 4/2019, σ. 8

3.1.1 Εκτίμηση «Αντικτύπου» στην Προστασία Δεδομένων και Προστασία Δεδομένων ήδη από τον σχεδιασμό

Ένα καινοτόμο στοιχείο που υιοθετεί ο ΓΚΠΔ για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα είναι η προσέγγιση της επεξεργασίας δεδομένων με βάση τον κίνδυνο, δηλαδή μια κινδυνοκεντρική προσέγγιση (risk-based approach).[83] Αυτή περιλαμβάνει τον καθορισμό των περιπτώσεων επεξεργασίας δεδομένων ανάλογα με τον βαθμό κινδύνου που ενέχουν για τα δικαιώματα των υποκειμένων των δεδομένων και την επιβολή ανάλογων υποχρεώσεων. Σύμφωνα και με την αιτιολογική σκέψη (76) του Κανονισμού *«η πιθανότητα και η σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων θα πρέπει να καθορίζονται σε συνάρτηση με τη φύση, το πεδίο εφαρμογής, το πλαίσιο, τους σκοπούς της επεξεργασίας. Ο κίνδυνος θα πρέπει να αξιολογείται βάσει αντικειμενικής εκτίμησης, με την οποία διαπιστώνεται κατά πόσον οι πράξεις επεξεργασίας δεδομένων συνεπάγονται κίνδυνο ή υψηλό κίνδυνο»*

Ο ΓΚΠΔ θέτει ως υποχρέωση του υπεύθυνου επεξεργασίας την εκπόνηση μελέτης, πριν προβεί σε οποιαδήποτε επεξεργασία για την εκτίμηση των επιπτώσεων στην προστασία δεδομένων από τις εν λόγω σχεδιαζόμενες πράξεις επεξεργασίας. [84] Η Εκτίμηση Αντικτύπου στην Προστασία Δεδομένων [Data Protection Impact Assessment–(εφεξής DPIA)] είναι μια διαδικασία που έχει σχεδιαστεί προκειμένου να περιγράψει την επεξεργασία των δεδομένων, να αξιολογήσει την αναλογικότητα και την αναγκαιότητα της εν λόγω επεξεργασίας και να συνδράμει στον εντοπισμό και στην διαχείριση των κινδύνων που σχετίζονται με την επεξεργασία των προσωπικών δεδομένων των υποκειμένων.[85]Ειδικότερα, σύμφωνα με το άρθρο 35 παρ. 1 του ΓΚΠΔ, η DPIA είναι υποχρεωτική σε περιπτώσεις όπου η επεξεργασία δεδομένων, ιδίως με χρήση νέων τεχνολογιών είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκείμενων των δεδομένων. [86] Επιπλέον, η DPIA

[83]Veil,2018,p.28
[84]Γιαννόπουλος, 2018,σ.96
[85]Βόρρας, 2023,σ.183
[86]Αλεξανδροπούλου- Αιγυπτιάδου,2021, σ.372

διενεργείται και βαρύνει πλέον ρητά τον υπεύθυνο επεξεργασίας, ο οποίος έχει την υποχρέωση να αξιολογήσει το σύνολο των παραμέτρων των κρίσιμων πράξεων επεξεργασίας πριν από την έναρξη τους, ώστε να εξασφαλιστεί η κατάλληλη και αποτελεσματική προστασία των υποκειμένων των δεδομένων. [87]

Κατά την ανάλυση των κινδύνων για τη συμμόρφωση με το άρθρο 25 παρ. 1 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας οφείλει τόσο να εντοπίζει τους κινδύνους που ενδέχεται να απειλήσουν τα δικαιώματα των υποκειμένων των δεδομένων σε περίπτωση παραβίασης των αρχών της ιδιωτικότητας, όσο και να εκτιμά την πιθανότητα και τη σοβαρότητα αυτών των κινδύνων, ώστε να εφαρμόζει κατάλληλα μέτρα για τον αποτελεσματικό μετριασμό τους. Επομένως, η διάταξη του άρθρου 25 παρ. 1 ενσωματώνει στις παραμέτρους της μια κινδυνοκεντρική προσέγγιση, η οποία με τη σειρά της, υπογραμμίζει τη στενή σχέση μεταξύ της υποχρέωσης για προστασία των δεδομένων από το σχεδιασμό και της διενέργειας Εκτίμησης Αντικτύπου για την Προστασία Δεδομένων. Άρα, η DPIA και η αρχή του PbD είναι δύο στενά συνδεδεμένες και συμπληρωματικές έννοιες, οι οποίες αλληλεπιδρούν στο πλαίσιο της προστασίας των προσωπικών δεδομένων και στην ανάπτυξη συστημάτων που επεξεργάζονται προσωπικές πληροφορίες. Μέσω των οποίων, οι υπεύθυνοι επεξεργασίας δύναται να διασφαλίσουν ότι έχουν εφαρμοστεί όλοι οι απαραίτητοι έλεγχοι προστασίας, ώστε οι προσωπικές πληροφορίες ενός ατόμου να προστατεύονται επαρκώς καθ' όλη τη διάρκεια του κύκλου ζωής τους. Είναι σημαντικό, ωστόσο, και πρέπει να τονιστεί ότι, οι δύο διατάξεις μπορεί να απολαμβάνουν ορισμένα κοινά χαρακτηριστικά, αλλά διαφέρουν, μεταξύ άλλων, στο γεγονός ότι η εφαρμογή του άρθρου 25 είναι απαραίτητη σε κάθε περίπτωση, σε αντίθεση με την DPIA η οποία εξαρτάται από ορισμένες προϋποθέσεις, ως ορίζονται στο άρθρο 35 του ΓΚΠΔ .[88]

[87] Ζωγραφόπουλος,2017,σελ. 41-43
[88]Καρκατζούνης, 2019

3.1.2 Προστασία δεδομένων ήδη από τον σχεδιασμό και ασφάλεια επεξεργασίας

Εξετάζοντας το άρθρο 25 παρ.1 ΓΚΠΔ, διαφαίνεται μια στενή σχέση ανάμεσα στην προστασία δεδομένων ήδη από τον σχεδιασμό και στην ασφάλεια της επεξεργασίας, διότι το νομικό πλαίσιο της διάταξης του άρθρου 25 φαίνεται να επηρεάζεται σημαντικά από την διατομεακή προσέγγιση στα ζητήματα προστασίας δεδομένων και στις τεχνολογίες ενίσχυσης της ιδιωτικότητας.[89] Το άρθρο 25 ΓΚΠΔ συμπληρώνει, επίσης, τις ευθύνες και τις υποχρεώσεις των υπεύθυνων επεξεργασίας, που ορίζονται στο άρθρο 24 ΓΚΠΔ και σε μεγάλο βαθμό, αποτελεί μια εξειδικευμένη πτυχή των υποχρεώσεών τους, που σχετίζεται με την αρχή της ασφάλειας.[90]

Το άρθρο 24 ΓΚΠΔ αποτελεί μια βασική διάταξη του Κανονισμού, καθώς ορίζει την ευθύνη του υπεύθυνου επεξεργασίας για την προστασία των προσωπικών δεδομένων των υποκειμένων. Αναλυτικότερα, το άρθρο 24 παρ.1 εδάφιο α' προβλέπει ότι *«ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό».* Διαφαίνεται, έτσι, ότι η ευθύνη του υπεύθυνου επεξεργασίας επιτείνεται, αφού εισάγεται ένα καθεστώς λογοδοσίας (accountability) [91] , που σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει όχι μόνο να εξασφαλίζει τη συμμόρφωσή του με τον κανονισμό, αλλά πρέπει να είναι και σε θέση να αποδείξει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύμφωνη με τις απαιτήσεις του κανονισμού, μέσω της υιοθέτησης και εφαρμογής τεχνικών και οργανωτικών μέτρων[92]. Επομένως, είναι πολύ σημαντικό, οι υπεύθυνοι επεξεργασίας να έχουν τη δυνατότητα να αποδείξουν την τήρηση των αρχών προστασίας δεδομένων, αλλά και να διαθέτουν τεκμηρίωση των εφαρμοζόμενων τεχνικών και οργανωτικών μέτρων, διασφαλίζοντας ότι αυτά τα μέτρα και εγγυήσεις

[89]Καρκατζούνης, 2019
[90]Ο.π.
[91] Labadie and Legner,2020,p.16
[92]Τζώρτζη, 2017, σ. 5

επιτυγχάνουν το επιθυμητό αποτέλεσμα.[93] Φαίνεται, έτσι ότι η ευθύνη του υπεύθυνου επεξεργασίας πλησιάζει κατ' ουσία την αντικειμενική ευθύνη και την ευθύνη από διακινδύνευση[94], δηλαδή δεν αρκεί να αποδείξει ότι «δεν φταίει», αλλά πρέπει να αποδεικνύει διαρκώς ότι κινείται εντός των ορίων που χαράσσει ο ΓΚΠΔ.[95]

Περαιτέρω, τα άρθρα 25 παρ.1 και 32 παρ. 1 ΓΚΠΔ επιτάσσουν να εξαρτάται η ένταση των ληπτέων μέτρων από τους υφισταμένους κινδύνους για τα δεδομένα, τη φύση, το πεδίο εφαρμογής, το είδος και τη διάρκεια της επεξεργασίας.[96]Είναι σημαντικό οι παράγοντες αυτοί να λαμβάνονται υπόψη από τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία από τη φάση σχεδιασμού των προϊόντων, υπηρεσιών και εφαρμογών, και να συνεχίζονται καθ' όλη τη διάρκεια του κύκλου ζωής τους.[97]

Ειδικότερα, το άρθρο 32 παρ.1προβλέπει την εφαρμογή ενός πλαισίου διαχείρισης κινδύνων και ασφάλειας των τεχνολογιών πληροφορικής, καθώς και μέτρων για τη μείωση των κινδύνων που αφορούν τα υποκείμενα, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία, διασφαλίζοντας έτσι την επαρκή και αποτελεσματική ασφάλεια των δεδομένων τους. Παραδοσιακά, ο όρος ασφάλεια δεδομένων χρησιμοποιείται για να περιγράψει τη συλλογή εργαλείων, μεθόδων και τεχνικών που αναπτύσσονται προκειμένου να επιτευχθούν οι στόχοι της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας. Όσον αφορά τον πρώτο στόχο, τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα, ο δεύτερος στόχος αφορά τα δεδομένα, τα οποία οφείλουν να είναι ακριβή, ακέραια και γνήσια, δηλαδή να μην είναι λανθασμένα, αλλοιωμένα ή μη ενημερωμένα και, ο τρίτος και τελευταίος στόχος, αφορά τα δεδομένα τα οποία πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Στη διεθνή σκηνή τα ως άνω στοιχεία είναι γνωστά με το ακρωνύμιο CIA, από τα

[93]Ο.π
[94] Σταθόπουλος,2004,σελ.314επ.
[95] Γιαννόπουλος,2018, σ.88
[96] Χριστοδούλου, 2020,σ.136
[97]Λουκάς, 2018, σελ.38 επ.

αρχικά των λέξεων Confidentiality, Integrity, Availability. [98]Οποιαδήποτε ενέργεια είτε τυχαία, είτε προμελετημένη, με δόλο ή αμέλεια προκαλέσει βλάβη, έστω σε ένα από τα ανωτέρω στοιχεία, συνίσταται ως «περιστατικό ασφαλείας». [99] Στο βαθμό, δε, που οδηγούν και σε διαρροή προσωπικών δεδομένων, τέτοια περιστατικά απασχολούν τον ΓΚΠΔ και την αρμόδια Εποπτική Αρχή ΑΠΔΠΧ.

3.1.3 Τεχνικά και Οργανωτικά μέτρα

Τα τεχνικά και οργανωτικά μέτρα μπορούν γενικά να θεωρηθούν ως οποιαδήποτε μέθοδος ή μέσο που δύναται να εφαρμοστεί από έναν υπεύθυνο επεξεργασίας κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η χρήση της λέξης *"κατάλληλα*" στη διάταξη του άρθρου 25 του ΓΚΠΔ σημαίνει ότι αυτά τα μέτρα και οι εγγυήσεις πρέπει να είναι επαρκή ώστε να επιτυγχάνεται ο στόχος, δηλαδή να εφαρμόζουν τις αρχές προστασίας δεδομένων με αποτελεσματικό τρόπο. Η αποτελεσματικότητα αποτελεί τον ακρογωνιαίο λίθο για την προστασία των φυσικών προσώπων και βρίσκεται στο επίκεντρο της έννοιας της προστασίας δεδομένων των υποκείμενων από τον σχεδιασμό.

Η επιλογή των εκάστοτε ενδεδειγμένων μέτρων θα πρέπει να γίνεται σύμφωνα με την αρχή της αναλογικότητας.[100] Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν τα αναγκαία και κατάλληλα μέτρα, προκειμένου να διασφαλιστούν τα δικαιώματα και οι ελευθερίες των υποκειμένων, των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία.

Το άρθρο 25 παρ. 1 δεν εξειδικεύει, ούτε προχωρά σε μια λεπτομερή και διεξοδική καταγραφή των τεχνικών και οργανωτικών μέτρων συμμόρφωσης. Ως εκ τούτου, τα μέτρα, τα οποία μπορούν να εφαρμοστούν από τον υπεύθυνο επεξεργασίας και να οδηγήσουν στη συμμόρφωση του με το άρθρο 25, εκτείνονται σε πολύ μεγάλη κλίμακα, όπως είναι η χρήση και εφαρμογή εξελιγμένων τεχνικών

[98]Κανέλλος, 2020, σ.35
[99]Τιντζογλίδου, 2022,σ. 86
[100]Χριστοδούλου,2020.σ.136

λύσεων, μέχρι και μια βασική εκπαίδευση του προσωπικού ενός οργανισμού. Το άρθρο 25 παρ. 1 προβλέπει ρητά τη τεχνική της ψευδωνυμοποίησης, ωστόσο, δεν αναφέρονται άλλα συγκεκριμένα τεχνικά ή οργανωτικά μέτρα, έτσι π.χ. θα μπορούσε να εφαρμοστεί μια πρόβλεψη συστημάτων που θα ανιχνεύει κακόβουλα λογισμικά, ή έγγραφες πολιτικές συμμόρφωσης.[101]Επίσης, μπορεί να καθιερωθούν συστήματα διαχείρισης απορρήτου και ασφάλειας πληροφοριών, προκειμένου οι εκτελούντες την επεξεργασία να εφαρμόζουν συγκεκριμένες πρακτικές ελαχιστοποίησης δεδομένων[102].

3.1.4 Η έννοια των «τελευταίων εξελίξεων»

Η έννοια των *«τελευταίων εξελίξεων»*, η οποία συναντάται και στο άρθρο 32 και στο άρθρο 25 του ΓΚΠΔ, χρήζει περαιτέρω ανάλυση, καθώς συνιστά μια δυναμική έννοια με πολύ μεγάλη σημασία για την ερμηνεία και εφαρμογή του ΓΚΠΔ. Η αναφορά της έννοιας αυτής υποχρεώνει τους υπεύθυνους επεξεργασίας να λαμβάνουν υπόψη την τρέχουσα τεχνολογική πρόοδο κατά τον καθορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων συμμόρφωσης. Αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να είναι διαρκώς ενήμεροι αναφορικά με το μεταβαλλόμενο και ραγδαίως εξελισσόμενο τεχνολογικό τοπίο. Πρέπει, επίσης, να διαθέτουν ένα επαρκές γνωστικό υπόβαθρό, το οποίο θα τους επιτρέπει να εφαρμόζουν και να επικαιροποιούν τα μέτρα και τις εγγυήσεις για να εξασφαλίσουν την αποτελεσματική προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Επομένως, η παρακολούθηση των τεχνολογικών εξελίξεων και της τεχνολογικής προόδου από τον υπεύθυνο επεξεργασίας, καθίσταται αναγκαίο στοιχείο, προκείμενου να επιτευχθεί η συμμόρφωση με το άρθρο 25 ΓΚΠΔ.

Το κριτήριο των «τελευταίων εξελίξεων» δε περιορίζεται μόνο στα τεχνολογικά μέτρα, αλλά ισχύει και για τα οργανωτικά μέτρα, η έλλειψη των οποίων, μπορεί

[101]Masoch, 2019,p.4
[102] Κατευθυντήριες γραμμές 4/2019, σ.7

να μειώσει ή να υπονομεύσει εντελώς την αποτελεσματικότητα μιας επιλεγμένης τεχνολογίας. Έτσι, η επικαιροποίηση εσωτερικών πολιτικών, η εκπαίδευση του προσωπικού σε θέματα σχετικά με τη τεχνολογία, την ασφάλεια και την προστασία δεδομένων, καθώς και αναφορικά με τις πολιτικές διακυβέρνησης και διαχείρισης της ασφάλειας πληροφοριακών συστημάτων είναι μόνο κάποια από τα μέτρα που μπορούν να εφαρμοστούν.[103]

Επομένως, οι προβλέψεις των άρθρων 25 και 32 του ΓΚΠΔ, είναι πολύ κρίσιμες, αναφορικά με τα τεχνικά και οργανωτικά μέτρα που πρέπει να λαμβάνονται από τον υπεύθυνο επεξεργασίας, καθώς αποσκοπούν στην εξασφάλιση της εφαρμογής τους για αποτελεσματική προστασία, λαμβάνοντας υπόψη τους υφιστάμενους κινδύνους για τα δεδομένα. Άρα, ο υπεύθυνος επεξεργασίας είναι αρμόδιος για την επιλογή των κατάλληλων διασφαλίσεων από τις διαθέσιμες τεχνολογίες, λαμβάνοντας υπόψη την τεχνολογική πρόοδο. Οφείλει, όμως να ελέγξει και να εξετάσει το κόστος των διασφαλίσεων αυτών ως μέρος της απόφασης του σε σχέση με τους κινδύνους για τα υποκείμενα των δεδομένων.

Αυτοί οι δύο παράγοντες, δηλαδή η πιο προηγμένη διαθέσιμη τεχνολογία και το κόστος εφαρμογής των μέτρων, πρέπει να ερμηνεύονται με τρόπο που να μειώνει επαρκώς τους υφιστάμενους κινδύνους, γιατί μόνο έτσι, θα επέλθει η απαιτούμενη και η απαραίτητη προστασία. [104] Άρα, η χρήση τεχνικών και οργανωτικών μέτρων ενισχύει την ασφάλεια από τον σχεδιασμό, εξασφαλίζοντας κατά αυτό τον τρόπο την αποτελεσματική αντιμετώπιση των κινδύνων και την εν τέλει τη προστασία των προσωπικών δεδομένων.

[103] Ο.π., σ.9
[104] European Data Protection Supervisor, Opinion 5/2018, p.6

ΚΕΦΆΛΑΙΟ 4ο ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΕΞ ΟΡΙΣΜΟΥ (PRIVACY BY DEFAULT)

4.1 Η έννοια της Privacy by Default

Η αρχή της προστασίας δεδομένων προσωπικού χαρακτήρα εξ ορισμού συνιστά μέρος της ευρύτερης αρχής της προστασίας δεδομένων προσωπικού χαρακτήρα από τον σχεδιασμό, και έτσι και οι δύο αρχές περιλαμβάνονται στη ίδια διάταξη του άρθρου 25. Στην πράξη, αυτές οι δύο έννοιες αλληλοσυμπληρώνονται κατά τρόπο αμοιβαίο.[105] Η ταυτόχρονη εφαρμογή τους ωφελεί τα υποκείμενα των δεδομένων, των οποίων τα προσωπικά δεδομένα υπόκεινται σε επεξεργασία. Επίσης, η προστασία δεδομένων εξ ορισμού, γνωστή και ως προστασία δεδομένων από προεπιλογή (Data Protection By Default), περιλαμβάνεται στις επτά θεμελιώδεις αρχές της προστασίας της ιδιωτικής ζωής από τον σχεδιασμό, σύμφωνα με την Ann Cavoukian, ζήτημα το οποίο αναλύθηκε εκτενώς ανωτέρω. Η αρχή αυτή έχει την έννοια ότι τα συστήματα επεξεργασίας προσωπικών δεδομένων πρέπει να έχουν προβλέψει και να διαθέτουν προεπιλεγμένες ρυθμίσεις, μέσω των οποίων να εξασφαλίζεται επαρκώς η προστασία των προσωπικών δεδομένων. Δύναται να επιτραπούν αποκλίσεις από την ως άνω υποχρέωση, μόνο, όμως, στην περίπτωση που τα υποκείμενα των δεδομένων, τα οποία αφορά η επεξεργασία, παρέχουν τη συγκατάθεση τους.

Κατά τη συζήτηση του ΓΚΠΔ προέκυψαν ερωτήματα σχετικά με την έκταση και το περιεχόμενο αυτής της υποχρέωσης. Ο Ευρωπαίος Επίτροπος υποστήριξε ότι η αρχή της προστασίας προσωπικών δεδομένων εξ ορισμού αποσκοπεί στην προστασία του υποκειμένου των δεδομένων σε καταστάσεις στις οποίες ενδέχεται να υπάρχει έλλειψη κατανόησης ή ελέγχου της επεξεργασίας των δεδομένων του, ιδίως σε τεχνολογικό πλαίσιο. Η ιδέα πίσω από την εν λόγω αρχή είναι ότι τα χαρακτηριστικά ενός συγκεκριμένου προϊόντος ή υπηρεσίας που παρεμβαίνουν

[105]Ιγγλεζάκης, 2018, σελ. 121επ

στην ιδιωτική ζωή περιορίζονται αρχικά σε οτιδήποτε είναι αναγκαίο για την απλή χρήση τους. Έτσι, το υποκείμενο των δεδομένων θα πρέπει κατ' αρχήν να έχει την επιλογή να επιτρέψει τη χρήση των προσωπικών του δεδομένων με ευρύτερο τρόπο. [106] Μια επιπλέον ερμηνεία που συνάδει με το πνεύμα της ρύθμισης θα μπορούσε να υποστηρίξει ότι χαρακτηριστικά προϊόντων και υπηρεσιών, τα οποία είναι φιλικά προς την ιδιωτικότητα θα πρέπει να ενεργοποιούνται αυτομάτως όταν αυτά ή/και αυτές χρησιμοποιούνται. [107] Αξιοσημείωτη είναι δε, και η σχέση που αναπτύσσεται ανάμεσα στη Privacy by Default και στις αρχές επεξεργασίας δεδομένων, καθώς υποχρεώνουν τον υπεύθυνο επεξεργασίας να λάβει μέτρα προκειμένου να διασφαλιστεί η εξ ορισμού τήρηση των αρχών του άρθρου 5 ΓΚΠΔ. Οι αρχές που, ιδίως, διέπουν την επεξεργασία προσωπικών δεδομένων και στις οποίες αποβλέπει η προστασία των δεδομένων εξ ορισμού είναι η αρχή της ελαχιστοποίησης των δεδομένων, καθώς και η αρχή του περιορισμού του σκοπού.[108]

4.2 Κυριότερα σημεία του Άρθρου25 παρ. 2 ΓΚΠΔ

Σύμφωνα, λοιπόν, με το άρθρο 25 παρ. 2 ΓΚΠΔ *«Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα*

[106] https://www.edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf , p.30 (par.181)
[107] Γιαννόπουλος, Μήτρου, Τσόλιας,2021,σ. 282
[108] Τζέλλης και Μυλώση, 2022 ,σ.129

προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων».

Αναλυτικότερα, η συνήθης χρήση του όρου «εξ ορισμού» στην επιστήμη των υπολογιστών, αναφέρεται στην προϋπάρχουσα ή προεπιλεγμένη τιμή μιας διαμορφώσιμης ρύθμισης που αντιστοιχεί είτε σε μια εφαρμογή υπολογιστή, είτε σε ένα πρόγραμμα ηλεκτρονικού υπολογιστή. Συνεπώς, κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ο εν λόγω όρος, αναφέρεται σε προεπιλεγμένες τιμές ρύθμισης ή σε επιλογές επεξεργασίας που καθορίζονται σε ένα σύστημα επεξεργασίας, όπως μια εφαρμογή λογισμικού ή σε ένα πρόγραμμα υπολογιστή ή σε μηχανισμό, που οδηγεί στην προσαρμογή της ποσότητας των προσωπικών δεδομένων που έχουν συλλεχθεί, της έκτασης της επεξεργασίας, της περιόδου αποθήκευσης ή της προσβασιμότητας στα προσωπικά δεδομένα.[109]

Περαιτέρω, η ως άνω διάταξη παραπέμπει στην αρχή της ελαχιστοποίησης των υπό επεξεργασία δεδομένων προσωπικού χαρακτήρα[110], η οποία αναφέρεται αφενός στον όγκο των δεδομένων, και αφετέρου στην ένταση και στην έκταση της επεξεργασίας, καθώς και στη χρονική διάρκεια τήρησης αυτών. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να διατυπώνει εκ των προτέρων τους συγκεκριμένους, σαφείς και νόμιμους σκοπούς για τους οποίους συλλέγονται και υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα. Τα μέτρα που εφαρμόζονται πρέπει εξ ορισμού να είναι κατάλληλα και επαρκή για να διασφαλίζεται ότι τα δεδομένα που υποβάλλονται σε επεξεργασία, είναι και τα απαραίτητα, ώστε να επιτευχθεί και ο συγκεκριμένος νόμιμος σκοπός της επεξεργασίας.[111]

Ομοίως, και στην περίπτωση της προστασίας δεδομένων εξ ορισμού, ο νομοθέτης δεν εξειδικεύει τα τεχνικά και οργανωτικά μέτρα τα οποία θα πρέπει να εφαρμοστούν και η αναφορά τους, ενδεχομένως, να παραπέμπει περισσότερο στην ασφάλεια των προσωπικών δεδομένων, ωστόσο, το ζητούμενο είναι ο

[109] Ο.π
[110] Άρθρο 5 παρ.1 στοιχ.γ ΓΚΠΔ
[111] Κατευθυντήριες γραμμές 4/2019, σ.13

υπεύθυνος επεξεργασίας να διασφαλίσει ότι τα δεδομένα δε θα τηρούνται πέραν του ελάχιστου αναγκαίου για τους σκοπούς της επεξεργασίας μέτρου. Ως εκ τούτου, όπως συμβαίνει και στην περίπτωση του άρθρου 25 παρ.1 του ΓΚΠΔ , την κατεύθυνση δίνει η αιτιολογική σκέψη 78 εδ. γ' ΓΚΠΔ, η οποία καθορίζει ένα γενικό πλαίσιο μέτρων, τα οποία δύναται να εφαρμόσει ο υπεύθυνος.[112]

4.2.1 Το εύρος των δεδομένων προσωπικού χαρακτήρα, ο βαθμός της επεξεργασίας ,η περίοδος αποθήκευσης και η προσβασιμότητα τους

Στο άρθρο 25 παρ. 2 εδάφιο β' αποτυπώνονται οι διαστάσεις της υποχρέωσης της ελαχιστοποίησης των δεδομένων για την εξ ορισμού επεξεργασία, οι οποίες εκτείνονται στο εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, στον βαθμό και στο διάστημα της επεξεργασίας, καθώς και στην προσβασιμότητα τους, δηλαδή τόσο από άποψη χρονικού διαστήματος, όσο και από άποψη ποσότητας. Ειδικότερα, σχετικά με *«το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται»*, ο υπεύθυνος επεξεργασίας οφείλει να εξετάζει, να ελέγχει, να αξιολογεί και να σταθμίζει το σύνολο, τις κατηγορίες, τους τύπους και το επίπεδο λεπτομέρειας των δεδομένων προσωπικού χαρακτήρα που είναι απαραίτητα και αναγκαία στοιχεία για τους σκοπούς της επεξεργασίας. Επομένως, η προεπιλεγμένη ρύθμιση πρέπει να περιορίζεται μόνο στα απαραίτητα και στα λιγότερο λεπτομερή δεδομένα για τον συγκεκριμένο σκοπό επεξεργασίας. Επειδή, λοιπόν, νομίμως, υποβάλλονται σε επεξεργασία μόνο τα απαραίτητα δεδομένα, κατοχυρώνεται ένα είδος «κυριαρχίας των δεδομένων», η οποία στοχεύει να διασφαλίσει την προστασία του υποκειμένου των δεδομένων.[113]

Επιπλέον, και η παράμετρος του «*βαθμού της επεξεργασίας*», έχει ως βασικό στοιχείο την αναγκαιότητα της επεξεργασίας των δεδομένων, ως εκ τούτου, οι πράξεις επεξεργασίας πρέπει να περιορίζονται μόνο σε ότι είναι απαραίτητο. Για τη πληρέστερη κατανόηση της ως άνω παραμέτρου, υπενθυμίζουμε ότι ως

[112]Γιαννόπουλος, Μήτρου,Τσόλιας,2021, σ.282
[113]Ιγγλεζάκης, 2018, σελ. 121επ.

επεξεργασία νοείται «*κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*».

Επιπροσθέτως, αναφορικά με την έννοια της περιόδου αποθήκευσης, ο υπεύθυνος επεξεργασίας οφείλει να περιορίζει το χρονικό διάστημα αποθήκευσης και διατήρησης των δεδομένων προσωπικού χαρακτήρα σε αυτό που είναι αναγκαίο για τον επιδιωκόμενο σκοπό. Στην περίπτωση, δε που τα δεδομένα προσωπικού χαρακτήρα δεν χρειάζονται πλέον για την εκπλήρωση του σκοπού της επεξεργασίας, τότε θα πρέπει εξ ορισμού είτε να διαγράφονται, είτε να ανωνυμοποιούνται. Επομένως, ο σκοπός της εκάστοτε επεξεργασίας καθορίζει και την διάρκεια του διαστήματος διατήρησης των δεδομένων. Η εν λόγω υποχρέωση συνδέεται κατά τρόπο άμεσο με την αρχή του περιορισμού της περιόδου αποθήκευσης που διατυπώνεται στο άρθρο 5 παρ. 1 στοιχ. ε' ΓΚΠΔ.[114]

Ο υπεύθυνος επεξεργασίας για να εφαρμόσει εξ ορισμού την παραπάνω υποχρέωση, οφείλει να έχει ενσωματώσει συστηματικές διαδικασίες για τη διαγραφή και την ανωνυμοποίηση των προσωπικών δεδομένων στην επεξεργασία του. Άρα, εάν η πραγμάτωση του σκοπού επεξεργασίας δεν καθιστά απαραίτητη την αποθήκευση των δεδομένων, αυτά με τη σειρά τους δε θα πρέπει να διατηρούνται. Ο υπεύθυνος επεξεργασίας θα πρέπει να μπορεί να αιτιολογεί αντικειμενικά στον βαθμό που είναι αναγκαίο οποιαδήποτε αποθήκευση και

[114]Άρθρο 5 παρ.1 στοιχ. εΓΚΠΔ: *«τα δεδομένα προσωπικού χαρακτήρα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων».*

διατήρηση προσωπικών δεδομένων, διότι έτσι θα συμμορφώνεται και με την αρχή της λογοδοσίας.[115],μια αρχή, η οποία, όπως αναλύθηκε και ανωτέρω, έχει ως βασικό περιεχόμενο το γεγονός ότι ο υπεύθυνος επεξεργασίας οφείλει από την μια να έχει θεσπίσει και να εφαρμόζει όλα τα απαραίτητα μέτρα για τη συμμόρφωσή του με τον ΓΚΠΔ και από την άλλη να είναι σε θέση να αποδεικνύει τη συμμόρφωση ενώπιον της εποπτικής και δικαστικής Αρχής.[116]

Ακολούθως, σχετικά με την παράμετρο της «*προσβασιμότητας*» των προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να επιβάλλει περιορισμούς με βάση μια εκτίμηση αναγκαιότητας, αναφορικά με το ποιος δύναται να έχει πρόσβαση, αλλά και σε σχέση με το είδος της πρόσβασης που μπορεί να απολαμβάνει σε δεδομένα προσωπικού χαρακτήρα. Είναι σημαντικό δε, ο υπεύθυνος επεξεργασίας να διασφαλίζει ότι τα δεδομένα αυτά είναι πράγματι προσβάσιμα, για όσους τα έχουν ανάγκη και, άρα, τα χρειάζονται λ.χ. όπως συμβαίνει σε καίριες και κρίσιμες καταστάσεις. Η εν λόγω υποχρέωση συνδέεται άμεσα με την ασφάλεια ως προς το σκέλος της εμπιστευτικότητας, και σύμφωνα με το άρθρο 5 παρ. 1 στοιχ. στ', τα δεδομένα προσωπικού χαρακτήρα «*υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων*».

4.2.2 Άρθρο 25 παρ. 2 εδάφιο. γ'

Το εδάφιο γ' της παραγράφου 2 του άρθρου 25 ΓΚΠΔ χρήζει περαιτέρω ανάλυσης, εξαιτίας της ευρείας διάδοσης και χρήσης του διαδικτύου, των μηχανών αναζήτησης και των μέσων κοινωνικής δικτύωσης από το σύνολο του πληθυσμού παγκοσμίως. Η πλέον προφανής επιταγή, ενδεχομένως και χρησιμότητα, της υπό συζήτηση παραγράφου συνίσταται στην υποχρέωση να διασφαλίζεται εξ ορισμού

[115]Κατευθυντήριες γραμμές 4/2019, σ. 15
[116]Πλιαβέσης,2019,σ.38

ότι τα προσωπικά δεδομένα ενός υποκειμένου δεν καθίστανται προσβάσιμα σε αόριστο αριθμό φυσικών προσώπων., δίχως την παρέμβασή του.[117]Η διάθεση των δεδομένων των υποκειμένων σε αόριστο αριθμό προσώπων ενδέχεται να προκαλέσει ακόμη μεγαλύτερη διασπορά των εν λόγω δεδομένων απ' ότι προοριζόταν σε αρχικό στάδιο. Αυτό, πρακτικά σημαίνει, ότι οι υπεύθυνοι επεξεργασίας, πρέπει εξ ορισμού να προσφέρουν την δυνατότητα στα υποκείμενα των δεδομένων να παρεμβαίνουν πριν από τη διάθεση των δεδομένων τους στο Διαδίκτυο.

Στη διάταξη γίνεται αναφορά στην έννοια της «*παρέμβασης*», που σημαίνει ότι απαιτείται θετική πράξη και όχι κάποιο είδος παθητικής συγκατάθεσης[118], ωστόσο η παρέμβαση μπορεί να ποικίλλει, με βάσει το πλαίσιο επεξεργασίας. Ως εκ τούτου δύναται να λαμβάνει ακόμη και τη μορφή συγκατάθεσης, η οποία θα επιτρέπει να καταστούν τα δεδομένα προσβάσιμα στη δημόσια σφαίρα ή ακόμη και να προβλέπει ρυθμίσεις απορρήτου, οι όποιες θα επιτρέπουν στα υποκείμενα των δεδομένων να ελέγχουν τη πρόσβαση στο ευρύ κοινό. [119] Είναι προφανές, ακόμη και εάν δεν γίνεται σχετική μνεία ότι, ο ευρωπαίος νομοθέτης στοχεύει στα ψηφιακά κοινωνικά δίκτυα, αφού ιδίως σε αυτό το πεδίο, οι προκαθορισμένες ρυθμίσεις (default settings) μπορούν να χρησιμοποιηθούν είτε για να καθοδηγήσουν είτε για να χειραγωγήσουν τις αντιλήψεις των προσώπων για τη καίρια σημασία και την προστασία της ιδιωτικότητας και τις αντίστοιχες επιλογές τους, επιδρώντας, έτσι με τη σειρά τους στον βαθμό προστασίας τους. Επομένως, η Privacy By Default σημαίνει εν προκειμένω ότι τα ψηφιακά προφίλ των χρηστών θα πρέπει εξ ορισμού να μην είναι προσβάσιμα δημοσίως, αντιθέτως, ο χρήστης θα πρέπει να προσδιορίζει κατά τρόπο ενεργό την «ορατότητά» τους (visibility).[120]

Ένα χρήσιμο παράδειγμα, το οποίο θα αναλυθεί στο επόμενο κεφάλαιο, ώστε να γίνει κατανοητή η αρχή της προστασίας των δεδομένων εξ ορισμού, προσφέρουν οι πλατφόρμες κοινωνικής δικτύωσης, όπως είναι το Facebook, Instagram, Twitter,

[117]Γιαννόπουλος, Μήτρου,Τσόλιας,2021 σ.282
[118]Ιγγλεζάκης, 2018, σελ.121επ.
[119]Κατευθυντήριες γραμμές 4/2019 σ.16
[120]Γιαννόπουλος, Μήτρου,Τσόλιας,2021, σ.282

οι οποίες θα πρέπει να ενθαρρύνονται να ορίζουν τις ρυθμίσεις των προφίλ των χρηστών, έτσι ώστε να προστατεύεται, όσο το δυνατόν περισσότερο, το ιδιωτικό απόρρητο, όπως όταν περιορίζεται από την αρχή η προσβασιμότητα στα προφίλ των χρηστών για να μην είναι προσβάσιμα εξ ορισμού από αόριστο αριθμό ατόμων.

ΚΕΦΑΛΑΙΟ 5ο ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΗΔΗ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΕΞ' ΟΡΙΣΜΟΥ

Στο παρόν κεφάλαιο, θα εξεταστούν δύο παραδείγματα που απορρέουν από τον ψηφιακό κόσμο. Το πρώτο εστιάζει στην προστασία των δεδομένων ήδη από τον σχεδιασμό, μέσα από τη χρήση κρυπτογράφησης από άκρο σε άκρο στην εφαρμογή ανταλλαγής μηνυμάτων WhatsApp, ενώ το δεύτερο παράδειγμα αφορά την προστασία των δεδομένων εξ ορισμού και επικεντρώνεται στα μέσα κοινωνικής δικτύωσης και ιδίως στη πλατφόρμα του Facebook.

5.1 Κρυπτογράφηση από άκρο σε άκρο του WhatsApp

Η χρήση των κινητών τηλεφώνων και, ειδικότερα, των έξυπνων κινητών (smartphones), έχει αναδειχθεί ως ο κυρίαρχος τρόπος επικοινωνίας στη σύγχρονη εποχή. Από τη στιγμή που τα smartphones έκαναν την εμφάνισή τους, η δημοτικότητά τους αυξήθηκε ραγδαία και έμελλε να αλλάξει ριζικά τον τρόπο με τον οποίο επικοινωνούν οι άνθρωποι. Αυτή η ραγδαία εξάπλωση οδήγησε στην ανάπτυξη πλήθους εφαρμογών ανταλλαγής μηνυμάτων, οι οποίες έγιναν γρήγορα δημοφιλείς, προσφέροντας νέες δυνατότητες για άμεση και εύκολη επικοινωνία. Από αυτές τις εφαρμογές, το WhatsApp που ανήκει στη Meta Inc έγινε η πιο δημοφιλής με πάνω από 5 δισεκατομμύρια χρήστες σε περισσότερες από 180 χώρες.[121]

Η εφαρμογή του WhatsApp δημιουργήθηκε το 2009 από τους από τους Jan Koum και Brian Acton, στοχεύοντας να καταστήσει την επικοινωνία και την ανταλλαγή πολυμέσων γρηγορότερη και πιο εύκολη. [122]Η εν λόγω εφαρμογή λειτουργεί μέσω σύνδεσης στο Διαδίκτυο και επιτρέπει στους χρήστες να παραμένουν σε επαφή με άτομα από τη λίστα επαφών τους, ενώ τους προσφέρει και άλλες δυνατότητες και επιλογές, όπως η δημιουργία ομάδων, κλήσεων, βιντεοκλήσεων και κοινή χρήση

[121]Pinaki Prasad Guha Neogi,2022,p.1
[122]Ο.π

αρχείων πολυμέσων, όπως, εικόνων, βίντεο, ήχων και εγγράφων. Η εφαρμογή επιτρέπει στους χρήστες να γνωρίζουν αν έχει σταλεί, παραδοθεί ή διαβαστεί ένα μήνυμα. Επίσης, η εφαρμογή δίνει τη δυνατότητα και την ελευθερία στον χρήστη να αποκλείσει ένα συγκεκριμένο άτομο στη λίστα επαφών του, στην περίπτωση που το επιθυμεί. Στα καίρια πλεονεκτήματα του WhatsApp είναι η χρήση της εφαρμογής χωρίς κάποιο κόστος και η διαθεσιμότητα του σε όλα τα δημοφιλή λειτουργικά συστήματα κινητής τηλεφωνίας. Έτσι, η δυνατότητα δωρεάν κλήσεων, απεριόριστων μηνυμάτων και η ανταλλαγή πολυμέσων, μαζί με μια εύκολη στη λειτουργία διασύνδεση, καθιστούν το WhatsApp προσιτό για κάθε λογής χρήστη, ακόμη, και για αρχάριους χρήστες, οι οποίοι είναι λιγότερο εξοικειωμένοι με την τεχνολογία.

Καθώς το WhatsApp εξελίχθηκε σε μία από τις πιο δημοφιλείς εφαρμογές επικοινωνίας παγκοσμίως η διασφάλιση της προστασίας της ιδιωτικότητας και της ασφάλειας των χρηστών έχει αποκτήσει θεμελιώδη σημασία. Οι χρήστες αναμένουν ένα εύλογο και υψηλό επίπεδο απορρήτου για τις προσωπικές και επαγγελματικές επικοινωνίες τους. Προκειμένου να ανταποκριθεί σε αυτές τις προσδοκίες, το WhatsApp εισήγαγε το 2014 την τεχνολογία κρυπτογράφησης από άκρο σε άκρο (End-to-End Encryption -E2EE), η οποία διασφαλίζει ότι τα δεδομένα που ανταλλάσσονται μεταξύ των χρηστών παραμένουν πλήρως προστατευμένα και απαλλαγμένα από υποκλοπές ή από μη εξουσιοδοτημένη πρόσβαση από τρίτα άτομα. [123]Η επικοινωνία των μερών καθίσταται πιο αξιόπιστη, καθώς με βάση τις αρχές της κρυπτογράφησης E2EE, τα δεδομένα που ανταλλάσσονται είναι ασφαλή κατά τη μεταφορά και μόνο ο αποστολέας και ο παραλήπτης μπορεί να αποκρυπτογραφήσει και να διαβάσει τα μηνύματα, ενώ ακόμα και η ίδια η εφαρμογή του WhatsApp δεν έχει τη δυνατότητα πρόσβασης σε αυτά τα δεδομένα. Έτσι, αυτή η τεχνική εγγυάται την ασφάλεια, την ιδιωτικότητα, την ακεραιότητα και το απόρρητο των επικοινωνιών των χρηστών.

Η τεχνική της κρυπτογράφησης μετατρέπει ένα μήνυμα απλού κειμένου σε μη αναγνώσιμο κώδικα, ο οποίος μπορεί να αποκρυπτογραφηθεί μόνο από όσους

[123]Endeley,2018,p.96

έχουν το μυστικό κλειδί. Η κρυπτογράφηση από άκρο σε άκρο είναι ένα σύστημα επικοινωνίας, το οποίο επιτρέπει μόνο στα επικοινωνούντα μέρη να έχουν πρόσβαση στα μηνύματα. Το hardware που είναι ενσωματωμένο σε τηλέφωνα επιτρέπει τις τυχαίες κλειδαριές και τα κλειδιά που κάνουν την κρυπτογράφηση από άκρο σε άκρο να λειτουργεί μόνο στις συσκευές που συμμετέχουν στη συνομιλία. Ένας υποκλοπέας δεν μπορεί να έχει πρόσβαση στα κρυπτογραφικά κλειδιά που απαιτούνται για την αποκρυπτογράφηση μιας συνομιλίας. Αξίζει να σημειωθεί ότι, δεν έχουν πρόσβαση στα εν λόγω κλειδιά, ακόμη και πάροχοι υπηρεσιών, όπως εταιρείες κινητής τηλεφωνίας, πάροχοι υπηρεσιών διαδικτύου, αλλά και προγραμματιστές εφαρμογών.[124]

Όσον αφορά το WhatsApp, το Πρωτόκολλο Σήματος ανοιχτού κώδικα επιτρέπει την κρυπτογράφηση από άκρο σε άκρο. Χρησιμοποιείται για την κρυπτογράφηση τόσο του κειμένου των μηνυμάτων, όσο και των φωνητικών κλήσεων, χρησιμοποιώντας μια ασύγχρονη μέθοδο υπό ένα κοινό κλειδί. Το Πρωτόκολλο επιλέχθηκε καθώς μπορεί να παρέχει μια αξιόπιστη/εύλογη άρνηση (Plausible deniability). Με τον όρο αυτό, νοείται ότι ο παραλήπτης ενός μηνύματος μπορεί να είναι σίγουρος από πού προέρχεται το μήνυμα, αλλά δεν μπορεί να αποδείξει την ταυτότητα του αποστολέα.[125]

Κάθε μέλος-συμμετέχων σε μια συνομιλία WhatsApp διαθέτει ένα μακροπρόθεσμο κλειδί ταυτότητας που είναι αποθηκευμένο στη μνήμη της συσκευής του και το οποίο χρησιμοποιεί για να υπογράψει ένα εφήμερο κλειδί. Αυτό το εφήμερο κλειδί ανταλλάσσεται μεταξύ των μελών για τον υπολογισμό ενός κοινόχρηστου μυστικού κλειδιού, συνήθως χρησιμοποιώντας τη μέθοδο ανταλλαγής κλειδιών Diffie-Hellman (D-H).[126] Η D-H επιτρέπει στους συμμετέχοντες να καθορίσουν από κοινού ένα κοινόχρηστο μυστικό κλειδί, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί για την κρυπτογράφηση μεταγενέστερων επικοινωνιών και να επιτρέψει μια ασφαλής επικοινωνία με τον

[124]Rastogi,Hendler, 2017,
[125]Ο.π.
[126]Ο.π.

άλλον χρήστη. Και τα δύο μέρη συμμετέχουν ταυτόχρονα στη δημιουργία του κοινού κλειδιού.

Είναι αξιοσημείωτο ότι, η κρυπτογράφηση από άκρο σε άκρο είναι μια από τις πιο συχνά χρησιμοποιούμενες τεχνολογίες για την ασφάλεια και την αποστολή πληροφοριών μέσω του διαδικτύου. [127]

5.2 Μέσα Κοινωνικής Δικτύωσης - Το Παράδειγμα του Facebook

Τα Μέσα Κοινωνικής Δικτύωσης συνιστούν ένα φαινόμενο μαζικής κουλτούρας, με το Facebook να συνιστά τη πλέον δημοφιλής πλατφόρμα που συνδυάζει μια σειρά διαδικτυακών εφαρμογών, αφού αποτελεί για τους χρήστες ένα διαδικτυακό μέσο διασκέδασης, πληροφόρησης, καθώς και επικοινωνίας με άλλους χρήστες. Με βάση μια έρευνα που διετέλεσε το Οικονομικό Πανεπιστήμιο Αθηνών, ένα μεγάλο ποσοστό των Ελλήνων χρηστών χρησιμοποιεί το Facebook επί καθημερινής βάσης, τόσο για τους λόγους που προαναφέρθηκαν, όσο και επειδή όχι μόνο το θεωρεί ως ένα απαραίτητο στοιχείο για την κοινωνική του ζωή, αλλά και επειδή το εμπιστεύεται σε σημαντικό βαθμό.[128] Αποτέλεσμα της χρήσης του Facebook είναι να δημιουργούνται ολοκληρωμένα ψηφιακά προφίλ των χρηστών του. Ωστόσο, αυτή η μαζική συγκέντρωση προσωπικών δεδομένων των χρηστών από μια ιδιωτική εταιρεία προκαλεί έντονες ανησυχίες και ζωηρό προβληματισμό αναφορικά με την προστασία των δεδομένων τους.

Η Διεθνής Ομάδα Εργασίας για την Προστασία Δεδομένων στις τηλεπικοινωνίες (Όμιλος Βερολίνου) ήταν από τις πρώτες που αντιμετώπισε ζητήματα απορρήτου στα κοινωνικά δίκτυα, έχοντας προτείνει τη δημιουργία ελάχιστων χαρακτηριστικών απορρήτου σε πλατφόρμες κοινωνικής δικτύωσης. [129] Στο

[127]Endeley,2018,p.96
[128]Πισκοπάνη, 2009, σ. 338
[129]Dix, 2010, σ.258

μνημόνιο της Ρώμης το 2008, η Ομάδα Εργασίας περιέγραψε λεπτομερώς τους κινδύνους που ελλοχεύουν από τα Μέσα Κοινωνικής Δικτύωσης, ιδίως από το Facebook, για την προστασία της ιδιωτικής ζωής και πρόσφερε οδηγίες για την αντιμετώπιση τους. Σύμφωνα με την εν λόγω ομάδα οι κοινότητες, όπως το Facebook προσφέρουν μια «ψευδαίσθηση οικειότητας» στους χρήστες, οι οποίοι συνήθως, καλούνται ή ενθαρρύνονται να χρησιμοποιούν τα πραγματικά τους ονόματα, όταν δημιουργούν τα ψηφιακά τους προφίλ. Το γερμανικό δίκαιο αναφέρει πως θα πρέπει να δίδεται τουλάχιστον η δυνατότητα χρήσης ψευδωνύμου. Η ομάδα εργασίας κάλεσε τόσο τις ρυθμιστικές αρχές, να εισάγουν μια ανάλογη επιλογή, αν δεν υπάρχει ήδη, όσο και τους παρόχους των εν λόγω υπηρεσιών να προτρέψουν τους χρήστες να χρησιμοποιούν τις υπηρεσίες κοινωνικής δικτύωσης με ψευδώνυμο. Ωστόσο, οι πάροχοι δεν είδαν την εν λόγω πρόταση με θετική ματιά, αλλά απεναντίας υποστήριξαν ότι η χρήση ψευδωνύμου θα αποτελέσει ανασταλτικό παράγοντα της ποιότητας των διαδικτυακών επικοινωνιών και θα δυσκολέψει την ταυτοποίηση επίδοξων cyber-stalkers. Είναι γεγονός, όμως, ότι ένα δίκτυο με ενσωματωμένο το ιδιωτικό απόρρητο, θα πρέπει να απαιτεί κατά την εγγραφή του χρήστη τα πραγματικά του στοιχεία, αλλά στο προφίλ του, το οποίο είναι ορατό από το σύνολο των διαδικτυακών του «φίλων» θα πρέπει να ενθαρρύνεται η χρήση ψευδωνύμου. [130]

Μια απόφαση που εμφατικά προβάλλει την ανασφάλεια της ιδιωτικότητας στις πλατφόρμες κοινωνικής δικτύωσης είναι η απόφαση που εξέδωσε το Διοικητικό Δικαστήριο του Αμβούργου, το οποίο αποφάνθηκε επί της διοικητικής διαφοράς που προέκυψε ανάμεσα στην εταιρία Facebook Ireland Limited και τον Επόπτη Προστασίας Προσωπικών Δεδομένων του Αμβούργου. [131] Μια χρήστης των υπηρεσιών της εταιρίας Facebook αντί για το πραγματικό της όνομα επέλεξε να χρησιμοποιεί ψευδώνυμο, με αποτέλεσμα να αποκλειστεί η πρόσβαση στο λογαριασμό της. Η «αποκλεισμένη» χρήστης αντέδρασε και απευθύνθηκε στον Επόπτη Προστασίας Προσωπικών Δεδομένων, ο οποίος υποχρέωσε την εταιρεία Facebook να δεχτεί το ψηφιακό προφίλ της αιτούσας με ψευδώνυμο και όχι με το

[130] 0.π.

[131] Άνθιμος,2016, σελ.70-71

πραγματικό της όνομα. Είναι σημαντικό να σημειωθεί ότι η απόφαση εκδόθηκε κατά της "Facebook Ireland Limited", η οποία αποτελεί την έδρα του Ομίλου Επιχειρήσεων Facebook για χώρες εκτός των ΗΠΑ και του Καναδά. Η εταιρία με τη σειρά της κίνησε διαδικασία ενώπιον των Διοικητικών Δικαστηρίων, ζητώντας την ακύρωση της απόφασης του Επόπτη. Το Διοικητικό Πρωτοδικείο αποφάσισε ότι το γερμανικό δίκαιο, επιτρέπει τη χρήση των δικτύων με ανώνυμο ή ψευδώνυμο τρόπο (άρθρο 13 παρ. 6 του γερμανικού νόμου περί τηλεπικοινωνιών) και βάσει του οποίου ο Επόπτης εξέδωσε την απόφασή του, ωστόσο στην υπό εξέταση περίπτωση δεν τυγχάνει εφαρμογής, επειδή πρέπει να εφαρμοστεί το δίκαιο του κράτους-μέλους, που είναι εγκατεστημένη η εταιρεία, και εν προκειμένω είναι το ιρλανδικό δίκαιο, και σύμφωνα με το οποίο, υφίσταται η υποχρέωση της χρήσης του πραγματικού ονόματος. Η εγκατάσταση της εταιρίας στη Γερμανία, κατά το σκεπτικό του δικαστηρίου, αφορά κυρίως διαφημιστικά ζητήματα και δεν επεξεργάζεται προσωπικές πληροφορίες. Έτσι, το Διοικητικό Δικαστήριο του Αμβούργου αποφάνθηκε, ότι η απόφαση του Επόπτη δεν πρέπει να εκτελεστεί και η εταιρία Facebook επιτρέπεται να αποφασίσει τη λειτουργία των λογαριασμών των χρηστών της μόνο με την χρησιμοποίηση των πραγματικών ονομάτων τους και όχι με τη χρήση ψευδωνύμων.[132]

Περαιτέρω, έντονο ενδιαφέρον παρουσιάζει το ζήτημα των προεπιλεγμένων ρυθμίσεων μιας πλατφόρμας κοινωνικής δικτύωσης. Στα μεγάλα κοινωνικά δίκτυα, όπως το Facebook, συνίσταται ως προεπιλογή ότι κάθε προφίλ είναι δημοσίως ορατό, δηλαδή οι προσωπικές πληροφορίες των χρηστών είναι δημόσια προσβάσιμες σε όλα τα μέλη της κοινότητας, εκτός εάν ο χρήστης περιορίσει την προβολή του σε κοινό το οποίο ο ίδιος έχει επιλέξει.[133] Ο Όμιλος Εργασίας του Βερολίνου επεσήμανε ότι σπανίως και, μόνο ένας μικρός αριθμός χρηστών θα προχωρήσει σε αλλαγές στις προεπιλεγμένες ρυθμίσεις, συμπεριλαμβανομένων των ρυθμίσεων απορρήτου. Οι προεπιλεγμένες ρυθμίσεις πρέπει να είναι φιλικές προς το απόρρητο και περιοριστικές, καθώς έτσι θα διαδραματίσουν ουσιαστικό ρόλο στην προστασία των προσωπικών δεδομένων των χρηστών, και κατ'

[132] Ο.π.
[133] Ιγγλεζάκης,2011,σελ.74-76

επέκταση στη προστασία του δικαιώματος τους στην ιδιωτική ζωή. Το ζητούμενο είναι κάθε χρήστης να είναι ελεύθερος μετά την εγγραφή του σε μια πλατφόρμα κοινωνικής δικτύωσης να ορίσει τον αριθμό των διαδικτυακών «φίλων» που επιθυμεί να έχουν πρόσβαση στα δεδομένα του. Οι πάροχοι υπηρεσιών, όμως, θεωρούν ότι έρχεται σε αντίθεση με το επιχειρηματικό τους μοντέλο, η περίπτωση που οι χρήστες στερούνται της δυνατότητας να επικοινωνήσουν εξ' αρχής με όλα τα μέλη της κοινότητας και ως εκ τούτου διαφωνούν με την παραπάνω προσέγγιση.[134]

Προκειμένου, λοιπόν, να επιτευχθεί η προστασία της ιδιωτικότητας, οι ρυθμίσεις απορρήτου των Υπηρεσιών Κοινωνικής Δικτύωσης (Privacy Settings) θα πρέπει να είναι εξαρχής εξαιρετικά περιοριστικές για τους χρήστες και στην περίπτωση που κάποιος χρήστης επιλέξει για τους δικούς του προσωπικούς λόγους να έχει το προφίλ του μεγαλύτερη δημοσιοποίηση, τότε θα πρέπει να προβεί από μόνος του σε αλλαγή των σχετικών ρυθμίσεων και να παραιτηθεί από την προεπιλεγμένη για αυτόν προστασία. Ωστόσο, η εν λόγω προεπιλογή της αυστηρής προστασίας των προσωπικών δεδομένων δεν πρέπει να θεωρείται ότι συνιστά απόρροια άκρατης πατερναλιστικής αντιμετώπισης των χρηστών των μέσων κοινωνικής δικτύωσης, αλλά ένα μέσο προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας τους.[135] Αν αναλογιστεί κανείς μόνο των αριθμό των ανηλίκων που έχουν πλέον πρόσβαση στα Μέσα Κοινωνικής Δικτύωσης, αλλά και πόσοι άλλοι χρήστες εγγράφονται στο Facebook χωρίς να διαθέτουν την κατάλληλη και επαρκή τεχνογνωσία για την προστασία των δεδομένων τους στο διαδικτυακό τόπο, μπορεί να συνειδητοποιήσει, πόσοι πολύ χρήστες τελικά κινδυνεύουν. Μέχρι και σήμερα τα Privacy Settings είτε δεν είναι τόσο γνωστά είτε είναι δύσχρηστα για μια μεγάλη μερίδα χρηστών, δημιουργώντας ένα χάσμα προστασίας της ιδιωτικότητας ανάμεσα στους ψηφιακά καταρτισμένους και εξοικειωμένους με το διαδίκτυο και με τα Μέσα Κοινωνικής Δικτύωσης και στους τεχνολογικά «αναλφάβητους». [136] Με τους μεν πρώτους να ονομάζονται

[134]Ο.π.

[135]Παναγοπούλου-Κουτνατζή,2012,σ.192

[136]Γεωργαλής,2020,σ.396

«ψηφιακοί ιθαγενείς» (digital natives),οι, δε, δεύτεροι να ονομάζονται «ψηφιακοί μετανάστες» (digital immigrants). [137] Είναι γεγονός, όμως, ότι στο Facebook θεσπίζεται ως αρχικό τεκμήριο για τον χρήστη ότι επιθυμεί τη διάδοση των πληροφοριών και όχι την προστασία τους. Και στην περίπτωση που επιθυμεί να περιορίσει τον κύκλο των προσώπων που έχουν πρόσβαση στο προφίλ του, τότε θα προβεί μόνος του στις απαιτούμενες ενέργειες. Η σημασία των Privacy Settings για την προστασία της ιδιωτικότητας είναι θεμελιώδης, και αυτό επειδή η ιδιωτικότητα στο πλαίσιο της πλατφόρμας του Facebook, θα μπορούσε να νοηθεί στο βαθμό που οι προσωπικές πληροφορίες και τα δεδομένα που ανταλλάσσονται παραμένουν στον κύκλο των χρηστών-«φίλων» που προσδιορίζει το υποκείμενο. [138]

[137] Ιγγλεζάκης,2011,σελ.74-76
[138] Γεωργαλής,2020,σ.396

ΚΕΦΑΛΑΙΟ 6ο Η ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΑΠΌ ΤΟΝ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΕΞ ΟΡΙΣΜΟΥ ΣΤΗΝ ΕΥΡΩΠΑΪΚΗ ΚΑΙ ΕΘΝΙΚΗ ΕΝΝΟΜΗ ΤΑΞΗ

6.1 Η Ευρωπαϊκή διάσταση της προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού

Όπως αναπτύχθηκε ανωτέρω, η νομοθεσία για την προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού βασίζεται στον ΓΚΠΔ, ο οποίος εισάγει τις αρχές της προστασίας δεδομένων εκ του σχεδιασμού και εξ ορισμού, ωστόσο οι εν λόγω αρχές εμφανίζονται, αν και όχι ρητά, και σε άλλες διατάξεις στο δίκαιο της Ευρωπαϊκής Ένωσης (εφεξής ΕΕ), με τον Ευρωπαίο νομοθέτη να αποδεικνύει, έτσι, τη σπουδαιότητα αυτών των αρχών για την προστασία της ιδιωτικότητας.

Είναι σημαντικό η εκκίνηση να δοθεί από την Σύμβαση 108 του Συμβουλίου της Ευρώπης του 1981 για την προστασία του ατόμου σε σχέση με την αυτοματοποιημένη επεξεργασία των δεδομένων προσωπικού χαρακτήρα, καθώς αποτελεί την πρώτη νομικά δεσμευτική διεθνής πράξη, η οποία προστατεύει το άτομο από τη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα και η οποία επιδιώκει να ρυθμίσει ταυτόχρονα τη διασυνορικαή ροή των εν λόγω δεδομένων. Στόχος της είναι να διασφαλίσει ότι κάθε φυσικό πρόσωπο προστατεύεται από την αθέμιτη χρήση των προσωπικών του δεδομένων, εξασφαλίζοντας, έτσι, το σεβασμό των δικαιωμάτων και των θεμελιωδών ελευθεριών του, και ιδιαίτερα του δικαιώματος στην ιδιωτική ζωή, έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων του.[139] Αρχικά, η εν λόγω συνθήκη παραλείπει να εισάγει στις διατάξεις της ειδικές απαιτήσεις για την προστασία δεδομένων από το σχεδιασμό και εξ ορισμού. Ωστόσο, η πρόταση του 2016 για την τροποποίηση και τον εκσυγχρονισμό της Σύμβασης, στοχεύει σε ένα ισχυρό νομικό πλαίσιο για τη διευκόλυνση της διασυνοριακής ροής δεδομένων, αποσκοπώντας στη επέκταση του πεδίου εφαρμογής της, στην ενίσχυση της προστασίας των δεδομένων και στη διασφάλιση της αποτελεσματικότητάς και της

[139]https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

αποδοτικότητας της Σύμβασης. Έτσι, το Μάιο του 2018, επικαιροποιήθηκε το κείμενο της Σύμβασης 108 του Συμβουλίου της Ευρώπης κα εισήγαγε ένα σύνολο διατάξεων, μεταξύ των οποίων, και το άρθρο 10 με τίτλο «Πρόσθετες υποχρεώσεις». Ειδικότερα, σύμφωνα με την παρ. 2 του άρθρου 10, οι υπεύθυνοι επεξεργασίας και, κατά περίπτωση, οι εκτελούντες την επεξεργασία εξετάζουν τις πιθανές επιπτώσεις της προβλεπόμενης επεξεργασίας δεδομένων στα δικαιώματα και στις θεμελιώδεις ελευθερίες των υποκειμένων των δεδομένων πριν από την έναρξη της επεξεργασίας και σχεδιάζουν την επεξεργασία δεδομένων κατά τρόπο ώστε να αποτρέπεται ή να ελαχιστοποιείται ο κίνδυνος επέμβασης στα δικαιώματα και στις θεμελιώδεις ελευθερίες των υποκειμένων. Στην παρ. 3 του άρθρου 10 γίνεται μνεία στην εφαρμογή τεχνικών και οργανωτικών μέτρων. Ειδικότερα, σύμφωνα με το γράμμα της διάταξης, κάθε συμβαλλόμενο μέρος προβλέπει ότι οι υπεύθυνοι επεξεργασίας, και, κατά περίπτωση, οι εκτελούντες την επεξεργασία, εφαρμόζουν τεχνικά και οργανωτικά μέτρα που λαμβάνουν υπόψη τις επιπτώσεις του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα σε όλα τα στάδια της επεξεργασίας των δεδομένων.[140]

Περαιτέρω, η Οδηγία 2002/58/ΕΚ «*για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών*» *(Οδηγία e-privacy)*[141] δεν αναφέρει ρητά και άμεσα στις διατάξεις της τις αρχές της προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού, ωστόσο γίνεται εμμέσως μνεία σε αυτές στην αιτιολογική σκέψη 30 της οδηγίας, η οποία διευκρινίζει ότι «*Τα συστήματα για την παροχή ηλεκτρονικών επικοινωνιακών δικτύων και υπηρεσιών θα πρέπει να σχεδιάζονται έτσι ώστε να περιορίζουν την ποσότητα των απαιτούμενων δεδομένων προσωπικού χαρακτήρα στο ελάχιστο δυνατό*». Πρόκειται, επομένως, για μια σύσταση στους παρόχους δημόσιων υπηρεσιών και προϊόντων ηλεκτρονικών επικοινωνιών να σχεδιάζουν τις εν λόγω

[140]https://search.coe.int/cm?i=09000016807c65bf
[141]Διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32002L0058

υπηρεσίες με τρόπο που να σέβεται και να τηρείται η αρχή της ελαχιστοποίησης των δεδομένων.

Εν συνεχεία, το 2017 η Ευρωπαϊκή Επιτροπή υπέβαλλε πρόταση Κανονισμού «*για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες*, γνωστός και ως κανονισμός e-Privacy, ο οποίος βρίσκεται ακόμη υπό παρατεταμένη διαβούλευση. Ο υπό συζήτηση κανονισμός θα καταργήσει την Οδηγία 2002/58/ΕΚ (Οδηγία e-Privacy), ενώ θα εξειδικεύσει και θα συμπληρώσει τον ΓΚΠΔ, καθώς τα δύο αυτά νομοθετήματα τελούν σε σχέση γενικού και ειδικού νόμου[142]. Έτσι, η ψήφιση του Κανονισμού e-Privacy, που θα αποτελεί ένα ενιαίο κείμενο με άμεση ισχύ σε όλα τα κράτη μέλη, θα συντελέσει στην ειδικότερη και αποτελεσματικότερη προστασία της ιδιωτικότητας των τελικών χρηστών. Σύμφωνα με το άρθρο 10 παρ. 1 της Πρότασης Κανονισμού της 10ης Ιανουαρίου 2017 «*Τα προϊόντα λογισμικού που διατίθενται στην αγορά και προσφέρουν τη δυνατότητα ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένης της ανάκτησης και παρουσίασης πληροφοριών στο διαδίκτυο, παρέχουν επιλογή που αποτρέπει την αποθήκευση πληροφοριών από τρίτους στον τερματικό εξοπλισμό του τελικού χρήστη ή την επεξεργασία πληροφοριών ήδη αποθηκευμένων σε αυτόν τον εξοπλισμό[143]*». Άρα, το εν λόγω άρθρο παρέχει στους τελικούς χρήστες την "επιλογή" να καθορίζουν μέσω των ρυθμίσεων του λογισμικού αν θα επιτρέπουν σε τρίτους να έχουν πρόσβαση ή να αποθηκεύουν πληροφορίες όσον αφορά τις συσκευές τους. Ωστόσο, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων με τη γνώμη 6/2017 θεώρησε ότι η διάταξη του άρθρου 10 δεν συνάδει με το άρθρο 25 παρ. 2 του ΓΚΠΔ και πρότεινε την αυστηροποίηση της διάταξης, η οποία δε θα προσφέρει απλώς την επιλογή, αλλά θα επιβάλλει την υποχρέωση στους παρόχους υλικού και λογισμικού να εφαρμόζουν προεπιλεγμένες ρυθμίσεις που προστατεύουν τις συσκευές των τελικών χρηστών από οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση ή αποθήκευση πληροφοριών στις συσκευές τους. [144]

[142]Κανέλλος, 2020,σ.121
[143]https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010
[144]EDPS, Opinion 6/2017, p.19

Στις 10 Φεβρουαρίου 2021 σημειώθηκε μια σημαντική εξέλιξη, καθώς το Συμβούλιο της Ευρωπαϊκής Ένωσης δημοσίευσε μια αναθεωρημένη πρόταση του Κανονισμού e-Privacy. Στην πρόταση αυτή, το άρθρο 10 της αρχικής εκδοχής του 2017, που αφορούσε τις ρυθμίσεις απορρήτου σε επίπεδο λογισμικού, έχει πλέον απαλειφθεί.[145]Αναμένουμε την τελική έκδοση του Κανονισμού e-Privacy, η οποία θα καταγράψει τις οριστικές ρυθμίσεις που αναφέρονται στα εν λόγω ζητήματα.

Ακολούθως, ο Κανονισμός (ΕΕ) 910/2014 για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (Κανονισμός e-IDAS) στοχεύει μέσω της θέσπισης νομοθετικού πλαισίου για τη ψηφιακή ταυτότητα, τόσο να διευκολύνει τις ασφαλείς διασυνοριακές συναλλαγές, όσο και να δημιουργήσει ένα πεδίο εμπιστοσύνης στις ηλεκτρονικές αλληλεπιδράσεις και στην προώθηση απρόσκοπτων ψηφιακών υπηρεσιών στην ψηφιακή ενιαία αγορά της ΕΕ. Αδιαμφισβήτητα, η παροχή τέτοιων υπηρεσιών καθιστά αναγκαία την επεξεργασία προσωπικών δεδομένων από τον πάροχο υπηρεσιών. Έτσι, ο κανονισμός, με το άρθρο 12 προβλέπει τη συνεργασία και τη διαλειτουργικότητα των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης μεταξύ των κρατών μελών της ΕΕ.

Ειδικότερα, στην παρ. 3 στοιχ. γ' του άρθρου 12 αναφέρεται ρητώς η προστασία από τον σχεδιασμό ως μια αρχή που πρέπει να υποστηρίζεται από τον πλαίσιο διαλειτουργικότητας e-IDAS.[146] Δηλαδή, η τεχνική εφαρμογή, η υποστήριξη των υπηρεσιών και τα διαδικαστικά και τεχνικά πρότυπα θα πρέπει να καθοδηγούνται από ένα κοινό πλαίσιο διαλειτουργικότητας, το οποίο θα εφαρμόζει την αρχή της προστασίας εκ του σχεδιασμού.

Τον Απρίλιο του 2024, κατόπιν παρατεταμένων διαπραγματεύσεων, η ΕΕ ενέκρινε τον Κανονισμό 2024/1183[147]για την τροποποίηση του κανονισμού (ΕΕ) 910/2014

[145]https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[146]https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32014R0910
[147]https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L_202401183

όσον αφορά τη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα. Σύμφωνα με την αιτιολογική σκέψη (9) του Κανονισμού 2024/1183 ο ΓΚΠΔ και, κατά περίπτωση, η οδηγία 2002/58/ΕΚ τυγχάνουν εφαρμογής στο σύνολο των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του κανονισμού 910/2014. Οι λύσεις βάσει του πλαισίου διαλειτουργικότητας που προβλέπεται στον κανονισμό 2024/1183 συμμορφώνονται, επίσης, με τους εν λόγω κανόνες.

Περαιτέρω, σύμφωνα με την αιτιολογική σκέψη (29)του Κανονισμού στόχος του είναι να παράσχει στον χρήστη ένα πλήρως κινητό, ασφαλές και εύχρηστο ευρωπαϊκό πορτοφόλι ψηφιακής ταυτότητας, το οποίο θα πρέπει να είναι ικανό να εξασφαλίσει το υψηλότερο επίπεδο προστασίας δεδομένων και ασφάλειας, ώστε τόσο η ηλεκτρονική ταυτοποίηση, όσο και η επαλήθευση της ταυτότητας να διευκολύνουν την πρόσβαση σε δημόσιες και ιδιωτικές υπηρεσίες ανεξαρτήτως από το που είναι αποθηκευμένα τα εν λόγω δεδομένα, δηλαδή είτε σε τοπικό επίπεδο, είτε σε λύσεις που βασίζονται στο υπολογιστικό νέφος.

Ειδικότερα, σύμφωνα με το άρθρο 5α παρ. 4 περ. α' και β' *«Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας παρέχουν στον χρήστη, κατά τρόπο φιλικό και διαφανή, τη δυνατότητα: α) με τρόπο ασφαλή, να ζητεί, να αποκτά, να επιλέγει, να συνδυάζει, να αποθηκεύει, να διαγράφει, να διαμοιράζεται και να προσκομίζει, υπό τον αποκλειστικό του έλεγχο, δεδομένα ταυτοποίησης προσώπου και, κατά περίπτωση, σε συνδυασμό με ηλεκτρονικές βεβαιώσεις χαρακτηριστικών, να προβαίνει σε επαλήθευση ταυτότητας έναντι βασιζόμενων μερών εντός διαδικτύου και, όπου αρμόζει, σε λειτουργία εκτός διαδικτύου, με σκοπό την πρόσβαση σε δημόσιες και ιδιωτικές υπηρεσίες, διασφαλίζοντας παράλληλα τη δυνατότητα επιλεκτικής γνωστοποίησης δεδομένων β) να δημιουργεί ψευδώνυμα και να τα αποθηκεύει κρυπτογραφημένα και τοπικά εντός του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας»*. Επομένως, ο νέος κανονισμός περικλείει ένα σύνολο βελτιωμένων μέτρων για την προστασία της ακεραιότητας και του απορρήτου των

χρηστών, τα οποία περιλαμβάνουν, μεταξύ άλλων, το δικαίωμα ψευδωνυμίας (άρθρο 5).

Ο Κανονισμός αναγνωρίζει τη σημασία της ανωνυμίας στο διαδίκτυο και θεσπίζει το δικαίωμα στους χρήστες να χρησιμοποιούν τοπικά αποθηκευμένα ψευδώνυμα, προσφέροντας τους με αυτό τον τρόπο ένα επίπεδο προστασίας της ιδιωτικότητας, ωστόσο, αυτό το δικαίωμα δύναται να περιοριστεί σύμφωνα με την εθνική ή ευρωπαϊκή νομοθεσία.

Επιπλέον, σύμφωνα με την αιτιολογική σκέψη (31) του Κανονισμού, τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας θα πρέπει να είναι ασφαλή από τον σχεδιασμό και να εφαρμόζουν εξελιγμένα χαρακτηριστικά ασφάλειας για την προστασία π.χ. από την κλοπή ταυτότητας και άλλων δεδομένων, αλλά και κάθε άλλης ενδεχόμενης κυβερνοαπειλής. Ο ευρωπαίος νομοθέτης αναφέρει ρητά ορισμένα τεχνικά μέσα, όπως την κρυπτογράφηση. Συγκεκριμένα, αναφέρει ότι η ασφάλεια θα πρέπει να περιλαμβάνει προηγμένες μεθόδους κρυπτογράφησης και αποθήκευσης, όπου η πρόσβαση και η αποκρυπτογράφηση μπορεί να πραγματωθεί μόνο από τον χρήστη.

6.2 Η Εθνική διάσταση της προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού

Ο Έλληνας νομοθέτης θα μπορούσε να χαρακτηριστεί υπό μία έννοια ως «πρόδρομος» της μετέπειτα εξέλιξης. Ήδη το 1999 με τον Νόμο 2774/1999 «*για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα*», αποτυπώνεται η αρχή της προστασίας της πληροφοριακής ιδιωτικότητας δια του σχεδιασμού, έστω και με έμφαση στην αρχή της ελαχιστοποίησης των προς επεξεργασία προσωπικών δεδομένων[148]. Ειδικότερα, το άρθρο 4 παρ.5 του ως άνω νόμου, το οποίο αντικαταστάθηκε με το άρθρο 5 παρ.4 του Ν. 3471/2006 που φέρει τον τίτλο «*Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα*

[148] Μήτρου, 2013, σ.18

των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997»ορίζει ότι «*Ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα*». Αντίστοιχη υπήρξε η στόχευση και το πνεύμα της ρύθμισης του Ν. 3979/2011 για την ηλεκτρονική διακυβέρνηση που προβλέπει συγκεκριμένα στο άρθρο 7 παρ. 3 ότι «*ο σχεδιασμός, η διαμόρφωση και η προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης πρέπει να γίνεται, λαμβάνοντας υπόψη το δικαίωμα προστασίας των προσωπικών δεδομένων και την ανάγκη διαμόρφωσης των συστημάτων και υπηρεσιών κατά τρόπο ώστε να διασφαλίζεται η επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα*». Επομένως, θα μπορούσε να διαπιστώσει κανείς ότι η προσοχή του Έλληνα νομοθέτη εστιάζει στην ελαχιστοποίηση του όγκου των απαιτούμενων προς επεξεργασία δεδομένων και σύμφωνα δε με την Αιτιολογική έκθεση του νόμου πρόκειται για «*ρητή εξειδίκευση της υποχρέωσης ελαχιστοποίησης των δεδομένων που τυγχάνουν επεξεργασίας από φορείς του δημοσίου τομέα, μία υποχρέωση που απορρέει εξάλλου από την αρχή της αναλογικότητας*».[149]

Επιπροσθέτως, σε διάστημα δέκα πέντε (15) μηνών μετά την έναρξη ισχύος του ΓΚΠΔ, εισήχθη στην εθνική έννομη τάξη ο ν. 4624/2019, ο οποίος, μετά την ψήφισή του και την κατάργηση, με το άρθρο 84 αυτού, του προϊσχύσαντος Ν. 2472/1997, αποτελεί ορόσημο στο δίκαιο της προστασίας των προσωπικών δεδομένων στην Ελλάδα[150]. Ο ν.4624/2019 στοχεύει, μεταξύ άλλων, να εκφράσει τόσο τη βούληση του Έλληνα νομοθέτη στα πεδία εκείνα που ο νομοθέτης του ΓΚΠΔ του καταλείπει διακριτική ευχέρεια υπό τη μορφή κάποιων «ρητρών ανοίγματος ή ρητρών ευελιξίας» όσο και να ενσωματώσει την Οδηγία 680/2016/ΕΕ, η οποία αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της προλήψεως, διερευνήσεως, ανιχνεύσεως ή διώξεως ποινικών αδικημάτων ή της

[149] 0.π.
[150] Παλαιολόγου και Πλιαβέσης, 2020, σ.1

εκτελέσεως ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.[151]

Ειδικότερα, το άρθρο 69 παρ. 1 και 2 του Ν 4624/2019 αναφέρεται στην αρχή της προστασίας των δεδομένων εκ του σχεδιασμού και εξ ορισμού αντίστοιχα[152], ενσωματώνοντας, έτσι, τις διατάξεις του άρθρου 20 της Οδηγίας 680/2016/ΕΕ, το οποίο φέρει τον τίτλο «Προστασία των δεδομένων εκ του σχεδιασμού και εξ ορισμού». Ως εκ τούτου, η ενσωμάτωση της εν λόγω Οδηγίας στο εθνικό νομικό πλαίσιο και η καθιέρωση του νέου πλαισίου λειτουργίας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η οποία αναδεικνύεται σε θεματοφύλακα των προσωπικών δεδομένων σε εθνικό επίπεδο συμπληρώνουν τη νέα νομοθεσία με τις σχετικές ρυθμίσεις.[153] Ο Ν. 4624/2019 καθορίζεται από μια μινιμαλιστική προσέγγιση[154],καθόσον λαμβάνει υπόψη τον διάλογο ανάμεσα στον ενωσιακό και τον εθνικό νομοθέτη.

[151] Παναγοπούλου,2024,σ.183

[152]«*Ο υπεύθυνος επεξεργασίας, τόσο κατά τον καθορισμό των μέσων επεξεργασίας όσο και κατά τον χρόνο της επεξεργασίας, λαμβάνει τα κατάλληλα μέτρα για την εφαρμογή των αρχών προστασίας των δεδομένων προσωπικού χαρακτήρα, όπως η ελαχιστοποίηση των δεδομένων, με αποτελεσματικό τρόπο, ώστε να διασφαλίζεται η συμμόρφωση με τις νομικές απαιτήσεις και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας λαμβάνει υπόψη την κατάσταση της τεχνολογίας, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας και σοβαρότητας για τα προστατευόμενα έννομα συμφέροντα του υποκειμένου των δεδομένων της επεξεργασίας. Ειδικότερα, τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία και τα συστήματα επεξεργασίας επιλέγονται και σχεδιάζονται σύμφωνα με την αρχή της ελαχιστοποίησης. Τα δεδομένα Προσωπικού Χαρακτήρα καθίστανται ανώνυμα ή ψευδωνυμοποιούνται όσο το δυνατόν ταχύτερα, στο μέτρο του δυνατού, σύμφωνα με τον σκοπό της επεξεργασίας.2. Ο υπεύθυνος επεξεργασίας εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίσει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι αναγκαία για κάθε συγκεκριμένο σκοπό της επεξεργασίας. Αυτό ισχύει για τον αριθμό των συλλεγόμενων δεδομένων, την έκταση της επεξεργασίας τους, την περίοδο αποθήκευσής τους και την προσβασιμότητα τους. Ειδικότερα, τα μέτρα πρέπει να διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα δεν γίνονται προσπελάσιμα με αυτοματοποιημένα μέσα σε αόριστο αριθμό προσώπων».*

[153]Γριβοκωστόπουλος, 2021, σ.29

[154]ΦερενίκηΠαναγόπουλουΚουτνάτζη,2019,σ.331

ΚΕΦΑΛΑΙΟ 7ο ΑΠΟΦΑΣΕΙΣ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΓΙΑ ΤΗΝ ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΗΔΗ ΑΠΟ ΤΟΝ ΣΧΕΔΙΑΣΜΟ

7.1 Απόφαση ΑΠΔΠΧ 31/2019

Η απόφαση 31/2019 [155] της ΑΠΔΠΧ αφορά καταγγελίες συνδρομητών του Οργανισμού Τηλεπικοινωνιών Ελλάδος Α.Ε. (ΟΤΕ), σύμφωνα με τις όποιες, παρά το γεγονός ότι είχαν εγγραφεί στο μητρώο αντιρρήσεων του άρθρου 11 παρ. 2 του νόμου 3471/2006, δηλώνοντας, έτσι, ότι δεν επιθυμούν να δέχονται διαφημιστικές κλήσεις, εξακολουθούσαν να είναι αποδέκτες τέτοιων κλήσεων από τρίτες εταιρίες για σκοπούς προώθησης προϊόντων και υπηρεσιών. Όπως διαπιστώθηκε, οι συνδρομητές εμφανίζονταν μεν ως εγγεγραμμένοι χρήστες στο μητρώο στην εσωτερική εφαρμογή πελατειακών σχέσεων του ΟΤΕ, ωστόσο οι τηλεφωνικοί αριθμοί τους δεν περιλαμβάνονταν στο μητρώο, που απέστειλε ο ΟΤΕ στις συνεργαζόμενες διαφημιστικές εταιρείες, με αποτέλεσμα οι συγκεκριμένοι πελάτες, εξακολουθούσαν να είναι αποδέκτες ανεπιθύμητων διαφημιστικών κλήσεων. Το εν λόγω ζήτημα ήταν απόρροια ενός τεχνικού προβλήματος στο σύστημα του ΟΤΕ. Πιο συγκεκριμένα, η εταιρεία καταχωρεί τα στοιχεία των συνδρομητών στο σύστημα διαχείρισης πελατών (CRM) Siebel, το οποίο συνδέεται με την ηλεκτρονική πλατφόρμα (portal) του ΟΤΕ. Η σύνδεση μεταξύ των δύο συστημάτων είχε μια δυσλειτουργία, με αποτέλεσμα να μην μεταφέρονταν κατά ορθό τρόπο οι πληροφορίες για ορισμένους συνδρομητές. Δηλαδή, στην περίπτωση που ένας συνδρομητής ήταν εγγεγραμμένος στο μητρώο αντιρρήσεων του συστήματος του ΟΤΕ και υπέβαλε αίτημά φορητότητας για τη μεταφορά της τηλεφωνικής τους σύνδεσης σε άλλο πάροχο, τα στοιχεία του διαγράφονταν και από τα δύο συστήματα, τόσο από το σύστημα Siebel, όσο και από το σύστημα portal. Στην περίπτωση, όμως που ακύρωνε αυτό το αίτημα, ενώ τα δεδομένα επανεγγράφονταν στο Siebel, δεν ενημερώνονταν σωστά στο portal λόγω ενός σφάλματος στον κώδικα του συστήματος του ΟΤΕ. Αυτό είχε ως απότοκο να επηρεαστούν περισσότεροι από 16.000 συνδρομητές και να συνεχίσουν να είναι

[155] https://www.dpa.gr/sites/default/files/2019-12/31_2019anonym%20%281%29.pdf

αποδέκτες ανεπιθύμητων κλήσεων. Ο ΟΤΕ μόλις ενημερώθηκε από την Αρχή προέβη στη διόρθωση του τεχνικού προβλήματος.

Σύμφωνα με το σκεπτικό της απόφασης, κάθε πάροχος καθίσταται υπεύθυνος επεξεργασίας για το σκοπό της τήρησης του μητρώου του άρθρου 11 παρ. 2 του Ν. 3471/2006, επομένως, στην υπό συζήτηση απόφαση πάροχος είναι ο ΟΤΕ. Στην προκειμένη περίπτωση η Αρχή εντόπισε παραβίαση της αρχής της ακρίβειας (άρθρο 5 παρ. 1 γ ΓΚΠΔ), καθώς, ο ΟΤΕ ως υπεύθυνος επεξεργασίας, όφειλε να λαμβάνει όλα τα εύλογα μέτρα, ώστε τα δεδομένα που τηρεί να είναι ακριβή αναφορικά με τους σκοπούς της επεξεργασίας.

Επιπλέον, σχετικά με τον τρόπο τήρησης του μητρώου του αρ. 11 διαπιστώθηκε ότι από την σχεδίαση του συστήματος προβλεπόταν ότι τα δεδομένα των συνδρομητών θα τηρούνταν σε δύο διαφορετικά συστήματα του ΟΤΕ. Για να είναι η σχεδίαση αυτή σύμφωνη με το άρθρο 25 του ΓΚΠΔ, θα όφειλε να έχει ενσωματώσει κατάλληλα και επαρκή τεχνικά μέτρα για να διασφαλίζεται η ακρίβεια των δεδομένων των συνδρομητών. Λ.χ. τέτοια μέτρα θα μπορούσαν να είναι ένας περιοδικός έλεγχος ακρίβειας, είτε δειγματοληπτικός, είτε και στο συνολικό αριθμό των συνδρομητών. Το γεγονός ότι, δεν είχε ληφθεί κανένα τέτοιο μέτρο εκ μέρους του ΟΤΕ, οδήγησε την Αρχή στην διαπίστωση ότι συνίσταται παραβίαση της σωστής τήρησης του μητρώου του άρθρου 11, ακόμα και όταν η μη ορθή τήρηση οφείλεται σε επιβεβαιωμένο τεχνικό πρόβλημα, καθώς συνεπάγεται α) παράβαση της αρχής της προστασίας των δεδομένων ήδη από τον σχεδιασμό και της αρχής της ακρίβειας κατά την επεξεργασία των προσωπικών δεδομένων των συνδρομητών και β) στέρηση από τους συνδρομητές του δικαιώματος τους να μην λαμβάνουν ανεπιθύμητες διαφημιστικές κλήσεις, ενώ θεωρούσαν ότι αυτό το δικαίωμα προστατεύεται. Έτσι, η Αρχή επέβαλλε το διοικητικό χρηματικό πρόστιμο ύψους 200.000 ευρώ για την εν λόγω παράβαση.

7.2 Απόφαση ΑΠΔΠΧ 34/2019

Η Αρχή με την υπ' αριθ. 34/2019[156] απόφαση διερεύνησε ορισμένες καταγγελίες φυσικών προσώπων συνδρομητών του ΟΤΕ, όπου και προέκυψε ότι, από το 2013 και μετέπειτα, εξαιτίας τεχνικού σφάλματος, δεν λειτουργούσε κατά ορθό τρόπο η διαγραφή από τις λίστες αποδεκτών των μηνυμάτων διαφημιστικού περιεχομένου του ΟΤΕ, για όσους παραλήπτες ασκούσαν αυτό το δικαίωμα μέσω του συνδέσμου "unsubscribe".[157] Αντιθέτως, οι εναλλακτικοί μηχανισμοί, δηλαδή μέσω τηλεφώνου και μέσω αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου, λειτουργούσαν χωρίς κανένα εμπόδιο. Ως αποτέλεσμα, περίπου 8.000 συνδρομητές προσπάθησαν χωρίς επιτυχία να διαγραφούν από τις λίστες αποδεκτών μηνυμάτων διαφημιστικού περιεχομένου. Το τεχνικό αυτό σφάλμα είχε ως αποτέλεσμα να υπονομεύσει τα δικαιώματα των συνδρομητών, παραβιάζοντας το άρθρο 21 παρ. 3 του ΓΚΠΔ, σύμφωνα με το οποίο όταν τα υποκείμενα των δεδομένων αντιτίθενται στην επεξεργασία των δεδομένων τους για σκοπούς άμεσης εμπορικής προώθησης, τα εν λόγω δεδομένα δεν υποβάλλονται πλέον σε επεξεργασία για αυτούς τους σκοπούς.

Σύμφωνα με τα στοιχεία του φακέλου της υπόθεσης, η Αρχή διαπίστωσε ότι ο ΟΤΕ δεν διέθετε επαρκή και κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίσει την ορθή λειτουργία του μηχανισμού "unsubscribe". Λ.χ. δεν είχε προβλέψει μια καθορισμένη διαδικασία, η οποία θα τον βοηθούσε να εντοπίσει και να διορθώσει τη μη ικανοποίηση του προβλεπόμενου από το άρθρο 21 του ΓΚΠΔ δικαιώματος εναντίωσης του υποκειμένου. Σε αυτή τη διαπίστωση συνηγορεί και το γεγονός ότι, ακόμη και κατόπιν αιτήματος ενός υποκειμένου των δεδομένων να εξαιρεθεί από τη λήψη διαφημιστικών μνημάτων, καμία σχετική ενέργεια δεν έλαβε χώρα εκ μέρους του ΟΤΕ, η οποία να προσανατολίζεται προς της κατεύθυνση αποκατάστασης αυτού του ζητήματος. Έτσι, η Αρχή διαπίστωσε

[156] https://www.dpa.gr/sites/default/files/2019-12/34_2019anonym%20%281%29.pdf
[157] Συμεωνίδου, 2017, σ.1

παράβαση των άρθρων 21 και 25 παρ. 1 του ΓΚΠΔ και επέβαλε στον ΟΤΕ διοικητικό πρόστιμο ύψους 200.000 ευρώ.

Με αυτές τις δύο αποφάσεις διαφαίνεται η αδήριτη ανάγκη οι υπεύθυνοι επεξεργασίας να λαμβάνουν με αμείωτη σοβαρότητα την υποχρέωση για ακριβή διαχείριση των δεδομένων των υποκειμένων και να διασφαλίζουν την προστασία τους από το στάδιο του σχεδιασμού. Είναι αξιοσημείωτο δε, ότι η Αρχή δεν αρκείται μόνο σε μια θεωρητική ανάλυση του άρθρου 25 του ΓΚΠΔ αλλά δίνει βαρύτητα στη ορθή και αποτελεσματική εφαρμογή τεχνικών και οργανωτικών μέτρων, με καταγραφή ορισμένων παραδειγμάτων συμμόρφωσης.[158]

7.3 Απόφαση ΑΠΔΠΧ 4/2022

ΗΑΠΔΠΧ εξέδωσε την υπ' αριθ. 4/2022[159] απόφαση, με την οποία επέβαλε σε τηλεπικοινωνιακό όμιλο επιχειρήσεων διοικητικές χρηματικές κυρώσεις συνολικού ύψους € 9.250.000 για παραβάσεις των κανονιστικών υποχρεώσεων, που πηγάζουν τόσο από τον ΓΚΠΔ, όσο και από τη νομοθεσία περί προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Αποτελεί μια απόφαση- σταθμό στην ιστορία της Αρχής, καθώς επιβλήθηκε το υψηλότερο διοικητικό πρόστιμο που έχει ποτέ διαταχθεί από την Αρχή μέχρι σήμερα, καθώς, επίσης, και το μεγαλύτερο πρόστιμο που έχει επιβληθεί από εποπτική αρχή του ΓΚΠΔ, κατόπιν παραβίασης δεδομένων, χωρίς να επικεντρώνεται κατά τρόπο αποκλειστικό στα μέτρα ασφαλείας.[160]

Αρχικά σύμφωνα με το ιστορικό της απόφασης, κατά την χρονική περίοδο από 1/9/2020 έως 5/9/2020 σημειώθηκε ένα ιδιαιτέρως σημαντικό περιστατικό διαρροής δεδομένων από κλήσεις συνδρομητών. Ειδικότερα, το αρχείο που διέρρευσε («απλό» αρχείο δεδομένων)περιείχε στοιχεία και πληροφορίες αναφορικά με την κίνηση των κλήσεων, τις οποίες ο τηλεπικοινωνιακός πάροχος κρατούσε για

[158]Βαμβακά, και άλλοι,2019
[159]https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf
[160] Βέρρας,2021, σ.576

διάστημα 3 μηνών προς εκπλήρωση δύο σκοπών. Ο πρώτος σκοπός ήταν η εξυπηρέτηση αιτημάτων των συνδρομητών που αντιμετώπιζαν διάφορες δυσλειτουργίες και βλάβες στο δίκτυο κινητής τηλεφωνίας τους, όπως είναι η απουσία ή η κακή ποιότητα σήματος. Στην συνέχεια, το αρχείο αυτό, εμπλουτίστηκε με απλά προσωπικά δεδομένα, όπως το οικονομικό πρόγραμμα, την ηλικία και το φύλο των συνδρομητών και διατηρήθηκε για 12 μήνες, αποσκοπώντας στην εκπλήρωση του δεύτερου σκοπού, που ήταν η εξαγωγή στατιστικών στοιχείων για τον καλύτερο σχεδιασμό του δικτύου κινητής τηλεφωνίας. Μετέπειτα, το συγκεκριμένο εμπλουτισμένο αρχείο πέρασε από μια διαδικασία τεχνικής ανωνυμοποίησης, μέσω της χρήσης ενός αλγορίθμου σε συνδυασμό με ένα κλειδί (salt key), το οποίο μεταβάλλεται κάθε τρεις μήνες. Προκειμένου να περιοριστεί ο κίνδυνος επαναταυτοποίησης των ανώνυμων δεδομένων, το χρονικό διάστημα διατήρησης τους κείται στους 12 μήνες. Μετά από την γνωστοποίηση της παραβίασης από τον ίδιο τον πάροχο, η ΑΠΔΠΧ προέβη σε εξέταση των συνθηκών υπό τις οποίες συνέβη το περιστατικό, εξετάζοντας τόσο τη νομιμότητα της διατήρησης των αρχείων που διέρρευσαν όσο και τα μέτρα ασφαλείας που εφαρμόστηκαν. Η αρχή με γνώμονα τα πραγματικά και νομικά ζητήματα που τέθηκαν υπόψη της χώρισε το σκεπτικό της απόφασης σε τρεις ενότητες. Στην πρώτη ενότητα εξετάζονται τα ζητήματα νομιμότητας, που αφορούν τον πρώτο σκοπό για τον οποίο ο πάροχος διατηρούσε το «απλό» αρχείο δεδομένων των συνδρομητών. Ειδικότερα, την Αρχή απασχόλησαν εκτενέστερα, η νομική βάση της βλαβοδιαχείρισης, αν η διενέργεια της εκτίμησης αντικτύπου που έγινε είναι σύμφωνη με τις απαιτήσεις του ΓΚΠΔ και τέλος, αν τηρήθηκε η αρχή της διαφάνειας. Στην δεύτερη ενότητα αναλύονται τα ζητήματα που σχετίζονται με τον δεύτερο σκοπό, για τον οποίο τηρήθηκε από τον πάροχο το εμπλουτισμένο αρχείο και πιο συγκεκριμένα το ζήτημα της διαδικασίας ανωνυμοποίησης του εν λόγω αρχείου. Η τρίτη και τελευταία ενότητα αφορά σε πιο γενικά ζητήματα συμμόρφωσης με τον ΓΚΠΔ, λ.χ. όπως είναι τα μέτρα ασφαλείας που έχουν ληφθεί από τον πάροχο, αλλά και την εξέταση της σχέσης των δύο εταιρειών, της COSMOTEκαι του ΟΤΕ.

Η Αρχή, κατόπιν εξέτασης των εν λόγω ζητημάτων, αποφάνθηκε ότι υπήρξαν παραβάσεις σε αρκετά άρθρα του ΓΚΠΔ. Συγκεκριμένα, διαπιστώθηκε παραβίαση της αρχής της νομιμότητας (άρθρα 5 και 6 του Νόμου 3471/2006) και της αρχής της διαφάνειας, λόγω πλημμελούς και ασαφούς ενημέρωσης των συνδρομητών (άρθρο 5 παρ. 1 περ. α',13-14 του ΓΚΠΔ). Επιπλέον, εντοπίστηκε παράβαση του άρθρου 35 παρ. 7 του ΓΚΠΔ λόγω ανεπαρκούς Εκτίμησης Αντικτύπου, σημειώνεται, εν προκειμένου ότι, ο πάροχος είχε διενεργήσει Εκτίμηση Αντικτύπου, η οποία όμως θεωρήθηκε πλημμελής από την Αρχή, επιβάλλοντας πρόστιμο αντίστοιχο με αυτό που θα επιδικαζόταν και στην περίπτωση που ο πάροχος δεν είχε διενεργήσει καθόλου Εκτίμηση Αντικτύπου. [161] Ακολούθως, εντοπίστηκε παράβαση του άρθρου 25 παρ. 1 του ΓΚΠΔ λόγω ελλιπούς εφαρμογής της διαδικασίας ανωνυμοποίησης, που όπως αποδείχθηκε από την Αρχή επρόκειτο ουσιαστικά για ψευδωνυμοποίηση. Παράλληλα, διαπιστώθηκε παράβαση του άρθρου 12 παρ. 1 του Νόμου 3471/2006, καθώς τα τεχνικά και οργανωτικά μέτρα ασφαλείας που έλαβε ο πάροχος δεν ήταν τα ενδεδειγμένα, ώστε να προστατευθεί η ασφάλεια των υπηρεσιών του, έτσι κρίθηκαν ανεπαρκή, ενώ σημειώθηκε και παράβαση του άρθρου 5 παρ. 2, σε συνδυασμό με τα άρθρα 26 και 28 του ΓΚΠΔ, λόγω μη κατανομής των ευθυνών και των αρμοδιοτήτων μεταξύ των δύο εταιρειών του ομίλου.

Αναφορικά με την παράβαση του άρθρου 25 παρ. 1 του ΓΚΠΔ, η Αρχή έκρινε ότι αυτό που η εταιρεία αντιλαμβανόταν ως ανωνυμοποίηση των δεδομένων, τόσο το «απλό», όσο και το «εμπλουτισμένο» αρχείο, ουσιαστικά αποδείχθηκε ότι αυτά ήταν εν τέλει «ψευδωνυμοποιημένα». Αναλυτικότερα, ο πάροχος ενημέρωσε τους συνδρομητές του ότι τα προσωπικά τους δεδομένα είτε θα διαγραφούν με τρόπο που θα επιτρέπει τη μη ανάκτηση τους, είτε θα χρησιμοποιηθεί η τεχνική διαδικασία της ανωνυμοποίησης, η οποία σημαίνει ότι τα προσωπικά στοιχεία τροποποιούνται με τέτοιο τρόπο, έτσι ώστε να μην είναι πλέον δυνατή η αναγνώριση της ταυτότητας του ατόμου. Ωστόσο, ως αποδείχθηκε, κατόπιν της εξέτασης των πραγματικών ζητημάτων από την Αρχή διαπιστώθηκε ότι δεν

[161] Βέρρας,2021, σ.579

εφαρμόστηκε η τεχνική της ανωνυμοποίησης, η οποία είναι μια μη αναστρέψιμη διαδικασία, αλλά η τεχνική της ψευδωνυμοποίησης. Η διαφορά αυτή είναι καίριας σημασίας, καθώς σύμφωνα με τον ΓΚΠΔ, η ψευδωνυμοποίηση επιτρέπει την αναγνώριση ενός ατόμου μέσω συμπληρωματικών πληροφοριών. Αυτό σημαίνει ότι τα δεδομένα που έχουν ψευδωνυμοποιηθεί εξακολουθούν να θεωρούνται προσωπικά δεδομένα και όχι ανώνυμα, και έτσι να υπόκεινται στις διατάξεις του ΓΚΠΔ. Επομένως, η λάθος χρήση των όρων μπορεί να έχει σοβαρές και επιζήμιες νομικές συνέπειες, καθώς η ψευδωνυμοποίηση επιβάλλει στον υπεύθυνο επεξεργασίας την τήρηση των υποχρεώσεων που προβλέπονται από τον ΓΚΠΔ, όπως η υποχρέωση ενημέρωσης. [162]

Η εν λόγω απόφαση σηματοδοτεί μια αλλαγή για την εν γένει πολιτική επιβολής κυρώσεων της εποπτικής αρχής και παρέχει αρκετά χρήσιμα συμπεράσματα. Δικαιολογημένα αποτελεί μια απόφαση εξέχουσας σημασίας για την εξέλιξη της νομολογίας της Αρχής υπό το καθεστώς του ΓΚΠΔ και απαράμιλλου ενδιαφέροντος για τον νομικό κόσμο.

7.4 Απόφαση ΑΠΔΠΧ 10/2024

Μια απόφαση που παρουσιάζει κατεξοχήν ενδιαφέρον για το ζήτημα της ασφάλειας της επεξεργασίας των προσωπικών δεδομένων είναι η υπ. Αριθ. 10/2024 [163] , σύμφωνα με την οποία η εταιρία «ΕΛΛΗΝΙΚΑ ΤΑΧΥΔΡΟΜΕΙΑ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ», (εφεξής ΕΛΤΑ) υπέβαλε στην ΑΠΔΠΧ, γνωστοποιήσεις περιστατικών παραβίασης που αφορούσαν, κατά πρώτον, κρυπτογράφηση λογισμικού στο σύστημα της εταιρίας, ως συνέπεια κακόβουλης επίθεσης από τρίτους, και κατά δεύτερον, διαρροή προσωπικών δεδομένων τα οποία, σε επόμενο χρόνο, δημοσιεύτηκαν στο σκοτεινό ιστό (Dark Web).Η Αρχή, κατόπιν εξέτασης της ανωτέρω αρχικής γνωστοποίησης, ζήτησε από τα ΕΛΤΑ, τόσο την περιγραφή των ενεργειών που έλαβαν χώρα αναφορικά με την διερεύνηση και

[162]Βόρρας, 2022,σ.23
[163]https://www.dpa.gr/sites/default/files/2024-04/10_2024%20anonym_0.pdf

την αντιμετώπιση του εν λόγω περιστατικού, όσο και κάθε σχετική πληροφορία και αναφορά που ενδεχομένως γνωρίζει. Τα ΕΛΤΑ, αρχικά, υπέβαλαν τεχνική έκθεση περιστατικού κυβερνοασφάλειας, σχετικά με τις διαδικασίες ενημέρωσης τους για το περιστατικό. Το αίτημα της Αρχής δεν ικανοποιήθηκε μόνο με αυτή την υποβολή, έτσι, στην συνέχεια ζήτησε από τα ΕΛΤΑ τις πολιτικές και τις διαδικασίες πληροφορικής και ασφάλειας πληροφοριών του φορέα, αλλά και το τρόπο με βάση τον οποίο εφαρμόστηκαν αυτές οι πολιτικές και οι διαδικασίες, ώστε να αντιμετωπιστεί το εν λόγω περιστατικό παραβίασης. Τα ΕΛΤΑ προσκόμισαν την πολιτική ασφάλειας συστημάτων και δεδομένων και την πολιτική προστασίας της ιδιωτικότητας από τον σχεδιασμό και εξ ορισμού.

Τα ΕΛΤΑ κλήθηκαν σε ακρόαση από την ΑΠΔΠΧ, η οποία λαμβάνοντας υπόψη το σύνολο των πραγματικών και νομικών ζητημάτων, έκρινε ότι έλαβαν χώρα παραβάσεις των υποχρεώσεων του υπεύθυνου επεξεργασίας κάτ. άρθρα 5 παρ. 1 στοιχ. στ' και 32 παρ. 1,2 και 4 ΓΚΠΔ. Αναλυτικότερα, η Αρχή εντόπισε απουσία διασφάλισης του περιορισμού της πρόσβασης στο σύστημα μόνο σε εξουσιοδοτημένα πρόσωπα, προσκρούοντας, έτσι, στο άρθρο 5 παρ. 1 στοιχείο στ. του ΓΚΠΔ και παραβιάζοντας τις θεμελιώδεις αρχές της ακεραιότητας και της εμπιστοσύνης. Επιπλέον, η Αρχή, εντόπισε ότι κατά πρώτον, δεν είχαν ληφθεί ούτε είχαν εφαρμοστεί επαρκή και κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας, σύμφωνα με όσα ορίζονται στο άρθρο 32 του ΓΚΠΔ. Και κατά δεύτερον, ότι δεν είχε εφαρμοστεί στην πράξη κατά ορθό και αποτελεσματικό τρόπο η πολιτική ασφαλείας της επεξεργασίας των δεδομένων που είχε εγκριθεί από το διοικητικό συμβούλιο και είχε υιοθετηθεί από τον υπεύθυνο επεξεργασίας, παραβιάζοντας, ως εκ τούτου το άρθρο 32 του ΓΚΠΔ. Συνάγεται, εκ των ανωτέρω, ότι τα ΕΛΤΑ δεν κατάφεραν να διασφαλίσουν την αξιοπιστία των συστημάτων, την ακεραιότητα των διαδικασιών, την αποτελεσματικότητα των τεχνικών και οργανωτικών μέτρων για την ασφάλεια της επεξεργασίας, απόρροια της οποίας είναι ένα ανεπαρκές επίπεδο ασφαλείας μπροστά στο πλήθος των ενδεχόμενων απειλών και κινδύνων που έχουν να αντιμετωπίσουν τα υποκείμενα των δεδομένων. Συνεπώς, η Αρχή επέβαλε στα ΕΛΤΑ διοικητικό πρόστιμο συνολικού ύψους 2.995.140 ευρώ.

Η απόφαση 10/2024 τονίζει τη καίρια σημασία της προστασίας των δεδομένων προσωπικού χαρακτήρα από τον σχεδιασμό και εξ ορισμού, από τους ενδεχόμενους κινδύνους που επιφυλάσσει η επεξεργασία τους. Επιπλέον, αναδεικνύει τον εξαιρετικά σημαντικό ρόλο και την ευθύνη του υπεύθυνου επεξεργασίας, ο οποίος οφείλει να τηρεί τόσο την αρχή της λογοδοσίας, η οποία λειτουργεί ως «μηχανισμός εγγύησης» αναφορικά με την τήρηση των αρχών που πρέπει να διέπουν την επεξεργασία των προσωπικών δεδομένων, όσο και ειδικότερα, την αρχή της νομιμότητας κατά την επεξεργασία των δεδομένων και να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποτελεσματική «θωράκιση» της ασφάλειας των προσωπικών δεδομένων και κατ' επέκταση της προστασίας των υποκείμενων των δεδομένων.[164]

[164] Παπακωνσταντίνου,2024,σ.461

ΚΕΦΑΛΑΙΟ 8ο ΑΔΥΝΑΜΙΕΣ ΚΑΙ ΠΡΟΚΛΗΣΕΙΣ ΤΟΥ ΑΡΘΡΟΥ 25 ΓΚΠΔ

Το άρθρο 25 ΓΚΠΔ αποτελεί μια φιλόδοξα σχεδιασμένη και καινοτόμα διάταξη, η οποία διαδραματίζει κομβικό ρόλο στη προσπάθεια γεφύρωσης του χάσματος ανάμεσα στις τεχνολογικές εξελίξεις και στο νομικό πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα[165]. Ωστόσο, αυτή η προσπάθεια είναι πιθανό να υπονομευθεί σημαντικά από μια σειρά αδυναμιών και προκλήσεων κατά την εφαρμογή των κανόνων του ΓΚΠΔ, διότι το νομικό πλαίσιο του κανονισμού είναι δαιδαλώδες, ασαφές και πολύπλοκο. Αρχικά, ο κανονισμός αποτελείται από ένα πλήθος διατάξεων, οι οποίες περιλαμβάνουν νομικές υποχρεώσεις, ωστόσο, η έλλειψη περαιτέρω καθοδήγησης σχετικά με την εκπλήρωση τους, δύναται να προκαλέσει ορισμένες δυσκολίες έως και αδυναμία συμμόρφωσης με τον κανονισμό. Οι δυσκολίες συμπεριλαμβάνουν, μεταξύ άλλων, την έλλειψη σαφήνειας αναφορικά με τις μεθοδολογίες και τις παραμέτρους, οι οποίες κατά βάση περιγράφουν βασικές στρατηγικές και αρχές σχεδιασμού, αλλά παραλείπουν να εστιάσουν στο πρακτικό πλαίσιο, δηλαδή πως δύναται να εφαρμοστούν ώστε να επιτευχθεί η οικοδόμηση και η λειτουργία ενός ολοκληρωμένου συστήματος προστασίας των δεδομένων κατά τον σχεδιασμό.[166] Επίσης, σημαντική είναι και η αδυναμία επίτευξης μιας σαφής και επιτυχής επικοινωνίας με όσους συνεργάζονται άμεσα για τον σχεδιασμό και την ανάπτυξη πληροφοριακών συστημάτων.[167]

Ειδικότερα, ο καθορισμός των υποχρεώσεων των υπεύθυνων επεξεργασίας και η πρακτική εφαρμογή τους αποτελεί ένα αρκετά περίπλοκο ζήτημα. Σε αυτό συνηγορεί και ο ΓΚΠΔ, ο οποίος δεν παρέχει κάποια καθοδήγηση ως προς τον ενδεδειγμένο τρόπο συμμόρφωσης σχετικά με τις διατάξεις του, παρά μόνο εστιάζει στο επιδιωκόμενο αποτέλεσμα, ως εκ τούτου εναπόκειται στη διακριτική ευχέρεια του υπεύθυνου ή του εκτελούντος την επεξεργασία να επιλέξει εκείνος το καταλληλότερο μέτρο συμμόρφωσης. Όπως εκτενώς αναλύθηκε ανωτέρω, το

[165] Καρκατζόυνης,2019,σ.13
[166] Λουκάς,2019,σ.51
[167] Bygrave,2017,p.105

άρθρο 25 ΓΚΠΔ αναφέρει στις διατάξεις του ότι ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, χωρίς, όμως, να διευκρινίζει πώς αυτό θα εφαρμοστεί στη πράξη, προσφέροντας του, έτσι μια εκτεταμένη αυτονομία και ανεξαρτησία στην επιλογή του καταλληλότερου μέτρου. Η εν λόγω αυξημένη αυτονομία στη πράξη εγκυμονεί κινδύνους και δημιουργεί ασάφεια, καθώς δύναται να γεννήσει αμφιβολίες και να εγείρει προβληματισμούς αναφορικά με το εάν έχουν πραγματωθεί όλες οι ενέργειες που απαιτούνται για να συμμορφωθεί με τον ΓΚΠΔ. Υπό το ίδιο πνεύμα ανησυχίας, απορρέει και το ερώτημα πως θα αξιολογηθεί η καταλληλότητα και η επάρκεια των τεχνολογικών και οργανωτικών μέτρων που επιλέγει ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, ώστε να συμμορφωθεί με τον ΓΚΠΔ. Για παράδειγμα, στην περίπτωση που προκύψει μια παραβίαση δεδομένων από έναν ιό ή από μια επίθεση hackers, από ποια οπτική θα εξεταστεί αυτή η παραβίαση, δηλαδή, θα γίνει έλεγχος αν υπήρχαν έτερα πιο ασφαλή, αξιόπιστα και αποτελεσματικά μέτρα, τα οποία θα μπορούσαν να είχαν εφαρμοστεί από τον υπεύθυνο επεξεργασίας ή θα θεωρηθεί ως ένα γεγονός ανωτέρας βίας; Και υπό το καθεστώς ποιων κριτηρίων θα εκτιμηθεί ότι δεν ευθύνεται ο υπεύθυνος επεξεργασίας για το γενεσιουργό γεγονός της ζημίας, προκείμενου να απαλλαγεί από το βάρος της ευθύνης;[168]

Επιπλέον, η ασάφεια και η πολυπλοκότητα της νομικής διατύπωσης του άρθρου 25 ΓΚΠΔ καθιστά δύσκολη την επικοινωνία όχι μόνο μεταξύ των νομοθετών και των αρχών προστασίας δεδομένων, αλλά και των επαγγελματιών που αναπτύσσουν συστήματα πληροφοριών. Θα μπορούσε να υποστηριχθεί ακόμη, ότι αυτή η νομική γλώσσα λειτουργεί ως κρυπτογράφηση για όσους δεν έχουν νομικές γνώσεις, εμποδίζοντας, έτσι, την ικανότητα του άρθρου 25 να παρακινήσει την κοινότητα των μηχανικών να εργαστούν προς την επιθυμητή κατεύθυνση.[169] Το κεντρικό ερώτημα είναι τι πραγματικά διακυβεύεται εάν η κοινότητα των νομικών μιλά για όρους όπως «απόρρητο», «προστασία δεδομένων» και « ανωνυμία». Μεταξύ τους είναι τις περισσότερες φορές αρκετά

[168]Βουλγαρίδης, 2018, σελ.48-51
[169]Ο.π.

ξεκάθαροι σχετικά με την έννοια των ως άνω όρων, αυτό, όμως, ενδέχεται να μην ισχύει στην εξωτερική επικοινωνία με τους μηχανικούς, οι οποίοι με τη σειρά τους και κατόπιν μη διευκρίνησης και επεξήγησης των εννοιών, επαναπροσδιορίζουν τους όρους καθιστώντας τους ουσιαστικά ασυμβίβαστους με τη νομική επιστήμη, αλλά και δυσνόητους στο ευρύ κοινό, δυσκολεύοντας τους τη κατανόηση και χρήση αυτών των όρων.[170] Προκειμένου να αντιμετωπιστεί αυτό το ζήτημα, θα πρέπει να διασφαλίζεται από την κοινότητα των νομικών ότι οι απαιτήσεις του άρθρου 25 ΓΚΠΔ μεταφράζονται σε μια γλώσσα που κατανοούν οι μηχανικοί. [171]

Ακολούθως, ο αντίκτυπος και η επίδραση του άρθρου 25 στην ανάπτυξη των πληροφοριακών συστημάτων είναι πιθανό να περιοριστεί λόγω του στενού πεδίου εφαρμογής του και της περιορισμένης εμβέλειάς του. Όπως εκτενώς αναλύθηκε ανωτέρω, σύμφωνα με τη διάταξη του άρθρου 25,οιαπαιτήσεις της προστασίας ήδη από τον σχεδιασμό και εξ ορισμού επιβάλλονται ρητά στους υπεύθυνους επεξεργασίας. Ωστόσο, δεν είναι ασφαλές και θα δημιουργούσε έντονο προβληματισμό να υποθέσουμε ότι οι βασικές αποφάσεις σχεδιασμού θα λαμβάνονται αποκλειστικά ή κυρίως από εκείνους που ενεργούν υπό την ιδιότητα του υπεύθυνου επεξεργασίας δεδομένων. Η ανεπάρκεια αυτή επιτείνεται από το γεγονός ότι το άρθρο 25 παρ. 1 ορίζει το στάδιο του σχεδιασμού ως τη στιγμή που ο υπεύθυνος επεξεργασίας αναλαμβάνει την ιδιότητα αυτή. Ωστόσο, το στάδιο αυτό μπορεί να μη συμπίπτει και να μην ισοδυναμεί στην κυριολεξία με τη στιγμή του σχεδιασμού και της κατασκευής ενός πληροφοριακού συστήματος επεξεργασίας δεδομένων. Είναι αξιοσημείωτο σε αυτό το σημείο να αναφερθεί ότι το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) με την απόφαση – σταθμό Google Spain[172] προέβη σε μια ευρεία ερμηνεία του όρου "υπεύθυνος επεξεργασίας" αποσκοπώντας στην προστασία των ατόμων σε σχέση με την επεξεργασία των δεδομένων τους, αλλά και η Ομάδα Εργασίας του άρθρου 29 με τις συστάσεις της ζητούσε την υποχρεωτικότητα της αρχής του PbD τόσο για σχεδιαστές και κατασκευαστές τεχνολογίας, όσο και για υπεύθυνους επεξεργασίας, οι οποίοι

[170]Pohle, 2019, p.134
[171]ibid,p.138
[172]GoogleSpain,par.32-40

αποφασίζουν για την απόκτηση και χρήση ΤΠΕ. [173] Υπό το ίδιο πνεύμα, ο νομοθέτης δεν έχει άγνοια επί αυτών των θεμάτων, αλλά γνωρίζει αυτές τις ελλείψεις. Σε αυτή την διαπίστωση συνηγορεί το προτελευταίο εδάφιο της αιτιολογικής σκέψης 78 του Κανονισμού, η οποία, όπως υποστηρίχθηκε και ανωτέρω, καλείται να καλύψει το ως άνω κενό. Ωστόσο, το εν λόγω σημείο πέραν του ότι βρίσκεται καλά κρυμμένο στο τέλος μιας μακράς αιτιολογικής σκέψης, είναι ασαφή και χρησιμοποιεί όρους πολύ λιγότερο αυστηρούς και επιτακτικούς, όπως είναι η φράση «*θα πρέπει να ενθαρρύνονται*», που χρησιμοποιείται για τους παραγωγούς προϊόντων, υπηρεσιών και εφαρμογών, συγκριτικά με τις αυστηρές νομικές απαιτήσεις που τίθενται στο άρθρο 25 ΓΚΠΔ.[174]

Ακολούθως, σύμφωνα με το τελευταίο εδάφιο της αιτιολογικής σκέψης 78 *«Οι αρχές της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού θα πρέπει επίσης να λαμβάνονται υπόψη στο πλαίσιο των δημόσιων διαγωνισμών»*. Αναμφίβολα, πρόκειται για μια εξαιρετικά σημαντική πρόβλεψη, που αποσκοπεί στη καθιέρωση της ασφάλειας επεξεργασίας δεδομένων ως ένα βασικό πρότυπο «industry standard» για την ανάπτυξη λογισμικού και εφαρμογών στο πλαίσιο των δημοσίων διαγωνισμών.[175] Ωστόσο, η διατύπωση της αιτιολογικής έκθεσης δεν καθιστά τη προστασία των δεδομένων από τον σχεδιασμό και εξ ορισμού ως απαραίτητη προϋπόθεση για τους δημόσιους διαγωνισμούς, αλλά αντιθέτως, είναι υπερβολικά ασαφής και γενική ως προς το βάρος που απαιτείται να δοθεί στις αρχές της προστασίας εκ σχεδιασμού και εξ ορισμού. [176]

Περαιτέρω, το άρθρο 25 διαδραματίζει σημαντικό ρόλο στη στήριξη και στην εφαρμογή πολλών άλλων διατάξεων του ΓΚΠΔ, αν και αυτό δεν διευκρινίζεται στην ίδια τη διάταξη. Για παράδειγμα, το άρθρο 83 παρ. 2 στοιχ. δ' ορίζει ότι κατά το καθορισμό της επιβολής διοικητικών προστίμων για παράβαση του κανονισμού, καθώς και σχετικά με το ύψος των εν λόγω προστίμων για κάθε εξατομικευμένη και μεμονωμένη περίπτωση λαμβάνεται δεόντως υπόψη, μεταξύ

[173]Μήτρου,2013,σ.20
[174]Bygrave,2017,p.118
[175]Καρκατζούνης, 2019
[176]Bygrave,2017,σ.117

άλλων, «*ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, λαμβάνοντας υπόψη τα τεχνικά και οργανωτικά μέτρα που εφαρμόζουν δυνάμει των άρθρων 25 και 32*» ως εκ τούτου, καθίσταται σαφές ότι η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξορισμού και η υποχρέωση για τήρηση της ασφάλειας της επεξεργασίας συνιστούν σημαντικό παράγοντα για την επιβολή ή μη διοικητικού προστίμου, αναπτύσσοντας, έτσι, μια ενδιαφέρουσα σχέση ανάμεσα στο άρθρο 83 και στο άρθρο 25 του ΓΚΠΔ.[177]

Επιπροσθέτως, το άρθρο 34 παράγραφος 1 ΓΚΠΔ απαιτεί από τον υπεύθυνο επεξεργασίας να κοινοποιεί αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα (data breach) στο υποκείμενο των δεδομένων, ωστόσο, σύμφωνα με την παρ. 3 στοιχ. α' του άρθρου 34, η ως άνω ανακοίνωση δεν απαιτείται στην περίπτωση που «*ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση*».

Επιπλέον, η διάταξη του άρθρου 6 ΓΚΠΔ συνιστά μια διάταξη κεφαλαιώδους σημασίας, καθώς αναπτύσσει το ζήτημα της νομιμότητας της επεξεργασίας. Πιο συγκεκριμένα, η επεξεργασία είναι σύννομη στην περίπτωση που συντρέχουν ορισμένες προϋποθέσεις, μεταξύ άλλων, όταν το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς. Η συγκατάθεση ανήκει στον σκληρό πυρήνα των δικαιωμάτων του υποκειμένου των δεδομένων και συναντάται και σε άλλα νομικά κείμενα, αποτελώντας μια βασική έκφραση της αρχής του πληροφοριακού αυτοπροσδιορισμού (άρθρο 9^{α} Σ).[178] Σύμφωνα με την παρ. 4 του άρθρου 6 ΓΚΠΔ, στην περίπτωση που συντελείται επεξεργασία για διαφορετικό σκοπό από αυτόν για τον οποίο συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, η οποία δεν βασίζεται στη συγκατάθεση του

[177]Καρκατζούνης, 2019
[178]Στεργιάδης,2020, σ.520

υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή ενός κράτους μέλους, ώστε να εξακριβωθεί αν η νέα επεξεργασία είναι συμβατή με τον αρχικό σκοπό, για τον οποίο συλλέγονται τα δεδομένα προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας λαμβάνει υπόψη, μεταξύ άλλων, την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

Μια πρόκληση που ανακύπτει και προκαλεί αναμφίβολα προβληματισμό είναι η εμφάνιση των «Μεγάλων Δεδομένων» (Big Data) και της επεξεργασίας των προσωπικών δεδομένων για άλλους σκοπούς, εκτός του αρχικού. Ο όρος «Μεγάλα Δεδομένα» αναφέρεται στις πρακτικές δημιουργίας και ανάλυσης τεράστιων συνόλων δεδομένων, τα οποία δύναται να περιλαμβάνουν προσωπικές πληροφορίες.[179]Ειδικότερα, είναι γεγονός ότι, η σύγχρονη εποχή χαρακτηρίζεται από την αλματώδη ανάπτυξη και χρήση των «Μεγάλων Δεδομένων», τα οποία προσφέρουν τεράστιες δυνατότητες επεξεργασίας σημαντικών προσωπικών πληροφοριών. Η ανάλυση αυτών των «Μεγάλων Δεδομένων» μπορεί να προκαλέσει βλάβη στα δικαιώματα και στην ελευθερία των φυσικών προσώπων, εγείροντας, έτσι, προβληματισμούς στα υποκείμενα, των οποίων τα δεδομένα αναλύονται. Για να διασφαλιστεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα γίνεται νόμιμα και με ασφάλεια, πρέπει να εφαρμόζεται το άρθρο 25 του ΓΚΠΔ. Αυτό σημαίνει ότι τα πληροφοριακά συστήματα πρέπει να διαθέτουν δικλείδες ήδη από τον σχεδιασμό και εξ ορισμού, οι οποίες να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε στοχευμένη και ασφαλή επεξεργασία, για να είναι δυνατή η τεκμηρίωση της νομιμότητας της περαιτέρω επεξεργασίας [180] . Άρα, έτσι θα προστατευθεί τόσο η ιδιωτική ζωή των υποκειμένων των δεδομένων, όσο και θα ενισχυθεί η εμπιστοσύνη τους στις εταιρείες και τους οργανισμούς που διαχειρίζονται τα δεδομένα τους, επιτρέποντας την περαιτέρω επεξεργασία των δεδομένων με διαφανή και νόμιμο τρόπο.

[179]Zarsky, 2017,p.996
[180] Καρκατζούνης,2019

ΕΠΙΛΟΓΟΣ

Στη σύγχρονη ψηφιακή εποχή, η προστασία των προσωπικών δεδομένων αποτελεί ένα σημαντικό ζήτημα, καθώς η τεχνολογική πρόοδος και η αυξανόμενη σύνδεση και εξάρτηση από τα πληροφοριακά συστήματα, ενισχύουν τις προκλήσεις στον τομέα της ασφάλειας και της ιδιωτικότητας. Οι δυνατότητες και τα όρια της τεχνολογίας διαδραματίζουν ολοένα και πιο σημαντικό ρόλο στην προσωπική και στην κοινωνική ζωή των ανθρώπων. Το διαδίκτυο και ο Παγκόσμιος Ιστός αναπτύσσονται και μεταβάλλονται συνεχώς τα τελευταία χρόνια, προσφέροντας πλήθος δυνατοτήτων και πλεονεκτημάτων αυξάνοντας όμως τις ανησυχίες και τους κινδύνους για τα δικαιώματα και τις ελευθερίες των ανθρώπων, με την ανάγκη για αποτελεσματικότερη προστασία των προσωπικών δεδομένων να γίνεται ακόμη πιο επιτακτική.

Ο Ευρωπαίος νομοθέτης δεν έμεινε με σταυρωμένα τα χέρια και με το άρθρο 25 του ΓΚΠΔ θέσπισε δύο νέες νομικές υποχρεώσεις, την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Όπως εκτενώς αναλύθηκε ανωτέρω, η πρώτη αρχή, αναφέρεται στη λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων κατά το στάδιο του σχεδιασμού ενός συστήματος επεξεργασίας, όπως ενός προϊόντος, μιας υπηρεσίας ή μιας εφαρμογής. Ενώ, η δεύτερη αρχή, αφορά στην εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων τα οποία εξασφαλίζουν πως εξ ορισμού υπόκεινται σε επεξεργασία μόνο τα προσωπικά δεδομένα τα οποία είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Στο πλαίσιο της προστασίας δεδομένων από τον σχεδιασμό οι υπεύθυνοι επεξεργασίας καλούνται να εκπληρώσουν ένα πολύ απαιτητικό έργο, καθώς, οφείλουν να εντοπίσουν και να μεταφράσουν τις νομικές απαιτήσεις του άρθρου 25 του ΓΚΠΔ σε τεχνικές λύσεις, εστιάζοντας την προσοχή τους στις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας και στους μηχανισμούς ασφάλειας πληροφοριών, και να τις ενσωματώσουν στα συστήματα, στις υπηρεσίες και στις εφαρμογές.[181]

[181] Λουκάς,2019,σ.51

Συμπερασματικά, η διάταξη του άρθρου 25 επιχειρεί να υλοποιήσει ένα δύσκολο και απαιτητικό εγχείρημα, αυτό της σύνδεσης δύο κόσμων, του τεχνολογικού και του νομικού κόσμου, αυτό από μόνο του την χαρακτηρίζει ως μια καινοτόμα και φιλόδοξη διάταξη. Ωστόσο, δεν είναι απαλλαγμένη από αδυναμίες, οι οποίες απαιτούν λεπτούς χειρισμούς, ορθές ερμηνείες και σαφής επικοινωνία όσων εργάζονται άμεσα με τον σχεδιασμό και την ανάπτυξη των πληροφοριακών συστημάτων. Προκειμένου να επιτευχθεί στην πράξη η προστασία των δεδομένων ήδη από τον σχεδιασμό, η οποία συντελεί στην ενδυνάμωση της προστασίας των δεδομένων προσωπικού χαρακτήρα των υποκειμένων, απαιτείται η σύγκλιση ανάμεσα σε τρεις συνιστώσες, δηλαδή της κανονιστικής, της επιχειρηματικής και της τεχνολογικής, οι οποίες μέσω της αλληλεπίδρασης των ρυθμιστικών αρχών, των υπεύθυνων επεξεργασίας και των σχεδιαστών των προϊόντων συντείνουν στην δημιουργία καθολικά αποδεκτών προτύπων, ελαχιστοποιώντας κατά το μέτρο του δυνατού την ανασφάλεια δικαίου που προκαλεί το άρθρο 25 ΓΚΠΔ. Η αντιμετώπιση των τεχνικών πτυχών της προστασίας δεδομένων ήδη από τον σχεδιασμό που θα καταφέρει να εξισορροπήσει από την μια την αποδοτικότητα μιας υπηρεσίας, ενός προϊόντος ή ενός συστήματος και από την άλλη την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα εξακολουθεί να αποτελεί ένα «ανοιχτό» ζήτημα, καθώς και ένα μεγάλο στοίχημα. Έτσι, η βελτίωση των υπαρχόντων εργαλείων και προσεγγίσεων, σε συνδυασμό με την ανάπτυξη και υιοθέτηση εξελιγμένων τεχνολογικών λύσεων θα μπορούσαν να προσφέρουν ικανοποιητικές λύσεις. Βρισκόμαστε σε αναμονή και με απαράμιλλο ενδιαφέρον παρακολουθούμε την εξέλιξη του φλέγοντος αυτού ζητήματος.

ΠΑΡΑΡΤΗΜΑ ΒΙΒΛΙΟΓΡΑΦΙΚΩΝ ΠΑΡΑΠΟΜΠΩΝ

Αγγλόφωνη Βιβλιογραφία- Αρθρογραφία

Acquisti, A.,2010, *The Economics of Personal Data and the Economics of Privacy*, pp.1-50. Διαθέσιμο σε https://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf (Τελευταία πρόσβαση 28/9/2024)

Brooks,S. Garcia, M.,Lefkovitz, N.,Lightman, S., Nadeau,E.,2017., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, National Institute of Standards and Technology, pp.1-25, Διαθέσιμο σε https://doi.org/10.6028/NIST.IR.8062 (τελευταία πρόσβαση 29/10/2024)

Burkert, H., 1997, *Privacy-enhancing technologies: typology, critique, vision*, A. Agre and M. Rotenberg (Eds.), Technology and Privacy: The New Landscape, Cambridge MA,pp. 871-880 Διαθέσιμο σε https://jolt.law.harvard.edu/articles/pdf/v11/11HarvJLTech871.pdf (τελευταία πρόσβαση 29/10/2024)

Bygrave, L., 2017,*Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements*, Oslo law review, pp.105-120, διαθέσιμο σε https://www.idunn.no/doi/10.18261/issn.2387-3299-2017-02-03#body-ref-AFN5 (τελευταία πρόσβαση 28/10/2024)

Cavoukian, A., 2010, *Privacy by design: The Definitive Workshop: Identity in the Information Society* 3(2), pp. 247-251, Διαθέσιμο σε 10.1007/s12394-010-0062-y (τελευταία πρόσβαση 29/10/2024)

Cavoukian, A., 2011,*Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, University of California, Santa Cruz. pp. 1-2

Διαθέσιμο σε https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf, (τελευταία πρόσβαση 29/10/2024)

Dix, A., 2010, *Built –in privacy –no panacea, but a necessary condition for effective privacy protection*, Springer, pp.257-265, διαθέσιμο σε Springerlink.com https://link.springer.com/article/10.1007/s12394-010-0045-z (τελευταία πρόσβαση 31/10/2024)

Endeley. R., 2018, *End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger*, Journal of Information Security, pp.95-99, Διαθέσιμο σεhttps://doi.org/10.4236/jis.2018.91008 (τελευταία πρόσβαση 6/1/2025)

Information and Privacy Commissioner of Ontario, 2018,*Seven Foundational Principles*, pp.1-2,διαθέσιμο σε https://www.ipc.on.ca/sites/default/files/legacy/2018/01/pbd-1.pdf (τελευταία πρόσβαση 19/10/2024)

Information Commissioner's office, 2023, *Privacy - Enhancing Technologies (PETs)*, pp. 1-66, Διαθέσιμο σε https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf,

Goldeberg, I., 2007, *Privacy Enhancing Technologies for the Internet III: Ten Years Later*, David R Cheriton School of Computer Science University of Waterloo,pp.1-14, διαθέσιμο σε https://www.cypherpunks.ca/~iang/pubs/pet3.pdf (τελευταία πρόσβαση 29/10/2024)

Kool, L. van Schoonhoven, B.; van Lieshout, M.; Vedder, A.H.; Fleurke, F.M., 2011, *Trusted Technology Eenonderzoeknaar de toepassingsvoorwaardenvoor Privacy by Design in de elektronischedienstverlening van de overheid*, Tilburg University, pp. 1-90 διαθέσιμο σε:https://pure.uvt.nl/ws/files/1396913/Vedder_Trusted_technology_120120_publishers_immediately.pdf (τελευταία πρόσβαση 27/9/ 2024)

Labadie C. and Legner,C.,2020, *Personal Data Protection Inside and Out-Integrating Data Protection Requirements in the Data Lifecycle,* Enterprise Modeling and Information Systems Architecture 15(9): 1-20 διαθέσιμο σε https://dl.gi.de/server/api/core/bitstreams/45675d5f-8a3c-47a0-8c04-90c60257c8fc/content (τελευταία πρόσβαση 30/10/2024)

London Economics, 2020, *Study on the Economic Benefits of Privacy –Enhancing Technologies (Pets),* Final Report to the European Commission, DG Justice, Freedom and Security pp. 1-259 διαθέσιμο σε https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf (τελευταία πρόσβαση 29/10/2024)

Masoch, D., 2019, *Implementing privacy by design in practice*, Fabian Privacy Legal, διαθέσιμο σε:https://privacylegal.ch/download/48/Implementing_Privacy_by_Design_in_practice.pdf?inline=true (τελευταία πρόσβαση 15/10/2024)

Michelakaki,C. and Vale S., 2023, *Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR*, The Future of Privacy Forum (FPF) διαθέσιμο σε: https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf (τελευταία πρόσβαση 8/1/2025)

NidhiRastogi, James Hendler, 2017, *WhatsApp security and role of metadata in preserving privacy*, pp.1-8, Rensselaer Polytechnic Institute, διαθέσιμο σε https://arxiv.org/pdf/1701.06817 (τελευταία πρόσβαση 6/1/2025)

Nieto, A., Rios, R., Lopez, J., Ren, W., Wang, L., Choo, K. K. R., & Xhafa, F., 2019, *Privacy-awaredigitalforensics*, pp. 1-39 Διαθέσιμο σε https://www.nics.uma.es/pub/papers/1777.pdf (τελευταία πρόσβαση 15/10/2024)

Pfitzmann, A. and Hansen, M., 2010, *Terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management* (Version v0.34 Aug. 10, σελ.1-98, διαθέσιμο σε https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf (τελευταία πρόσβαση 29/10/2024)

Pohle, J., 2019, *Security by Design/Privacy and Data Protection by Design Privacy and Data Protection by Design: A Critical Perspective* ,Building Common Approaches for Cybersecurity and Privacy in a Globalized World, pp.134-141διαθέσιμο σε https://www.researchgate.net/publication/338209541_Privacy_and_Data_Protection_by_Design_A_Critical_Perspective (τελευταία πρόσβαση 29/10/2024)

Pinaki Prasad Guha Neogi, 2022, *A Dive into WhatsApp's End-to-End Encryption*, Dept. of Computer Science, School of ENCS, pp.1-6,διαθέσιμο σε https://arxiv.org/pdf/2209.11198 (τελευταία πρόσβαση 6/1/2025)

Rubinstein, I.,2012, *Regulating Privacy by Design.* Berkeley Technology Law Journal, Vol. 26,pp. 1409 επ., Διαθέσιμο σε SSRN: http://ssrn.com/abstract=1837862 (τελευταία πρόσβαση 29/10/2024)

Schwaab, J., 2010, *Privacy by Design Resolution*,32nd International Conference of Data Protection and Privacy Commissioners, διαθέσιμο σε https://www.schwaab.ch/wp-content/uploads/2013/09/Resolution+on+Privacy+by+Design.pdf (τελευταία πρόσβαση 30/10/2024)

Sweeney, L.,2000, *Simple Demographicς Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, pp.1-34 https://dataprivacylab.org/projects/identifiability/paper1.pdf (τελευταία πρόσβαση 29/10/2024)

Veil, W., 2018, *The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Ptotection Law*, Consumer Law e-Joyrnal, pp.1-28 διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305056 (τελευταία πρόσβαση 28/10/2024)

Zarsky, T., 2017, *Incompatible: The GDPR in the Age of Big Data,* Seton Hall Law Review, Vol,47 No.4(2),pp 995-1020, διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646 (τελευταία πρόσβαση 28/10/2024)

Ελληνική Βιβλιογραφία-Αρθρογραφία

Αλεξανδροπούλου- Αιγυπτιάδου, Ε., 2021, *«Σταθμίσεις συμφερόντων και νομοθετικές επιλογές στον Γενικό Κανονισμό Προστασίας Δεδομένων»*, ΔiMEE3/2021,σελ. 367-376

Άνθιμος, Α., 2016,*Προτιμήσεις και ανωνυμία στα κοινωνικά μέσα δικτύωσης - Με αφορμή δύο αποφάσεις γερμανικών δικαστηρίων*, ΣΥΝ, 114/2016, σελ. 70 - 71

Βαμβακά, Ε., Κωνσταντίνου, Σ., Τζιβιέρης, Ε., 2019,*Πρόστιμο 400.000€ της ΑΠΔΠΧ στον ΟΤΕ: Ένας σχολιασμός*, διαθέσιμο σε https://homodigitalis.gr/posts/4379/ (τελευταία πρόσβαση 25/10/2024)

Βέρρας Δ., 2021, *Παρατηρήσεις στην Απόφαση ΑΠΔΠΧ 4/2022. Μια απόφαση – σταθμός για την νομολογία της ΑΠΔΠΧ*, ΔiMEE, 4/2021, σελ. 576 – 581

Βουλγαρίδης, Σ., 2018, *Συμμόρφωση με τον ΓΚΠΔ: Δυσκολίες και ευκαιρίες για την επιχείρηση*, ΣΥΝ, 1/2018, σελ. 48 - 51

Βόρρας, Α., 2022, *Υψηλές κυρώσεις στο ρυθμιστικό περιβάλλον για την προστασία των προσωπικών δεδομένων*, ΣΥΝ, 150/2022, σελ. 22 – 24

Γεωργαλής, Φ-Ε, 2020, *Η ιδιωτικότητα στο Facebook μετά τον Γενικό Κανονισμό για την Προστασία Δεδομένων*, ΔiMEE, 3/2020, σελ. 395 – 401

Γιαννόπουλος, Γ., 2018,*Εισαγωγή στη Νομική Πληροφορική –Μια πρώτη προσέγγιση της σχέσης δικαίου και νέων τεχνολογιών*, Αθήνα: Νομική Βιβλιοθήκη

Γιαννόπουλος, Γ., Μήτρου, Λ., Τσόλιας, Γ.,επ. Μενουδάκος Κ. , Κοτσαλής Λ., *Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) – Νομική διάσταση και πρακτική εφαρμογή*, 2021, Αθήνα :Νομική Βιβλιοθήκη

Γριβοκωστόπουλος, Ι., 2021, *Κριτική ανάλυση του Ν. 4624/2019,* Επιθεώρηση Δικαίου Πληροφορικής, σελ. 1-24 διαθέσιμο σε https://ejournals.lib.auth.gr/infolawj/(τελευταία πρόσβαση 15/9/2024)

Δαντόγλου, Π.Δ., 2012, *Ατομικά Δικαιώματα*, Αθήνα-Θεσσαλονίκη, Εκδόσεις Σάκκουλα

Ζωγραφόπουλος, Δ., 2017,*Η υποχρέωση διενέργειας εκτίμησης αντικτύπου (Data protection impact assessment-DPIA) στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR)*, Συνήγορος,τ.120/ 2017, σελ. 41-43

Ιγγλεζάκης,Ι., 2018, *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679)-Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων*, Θεσσαλονίκη: 2η έκδοση, Εκδόσεις Interactive

Ιγγλεζάκης, Ι.,2013, *Προστασία Δεδομένων προσωπικού χαρακτήρα από τον σχεδιασμό (dataprotectionbydesign) και εξ' ορισμού (dataprotectionbydefault),* Συνήγορος τ.96/2013, σελ.76-78

Ιγγλεζάκης, Ι., 2011, *Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης - Σκιαγράφηση των ζητημάτων προστασίας της ιδιωτικότητας και αναζήτηση λύσεων - Μέρος 1ο*,ΣΥΝ, 84/2011, σελ. 74 - 76

Κανέλλος, Λ., 2020, *The GDPR Handbook, Για DPOs, Επιχειρήσεις & Οργανισμούς*, Αθήνα: Νομική Βιβλιοθήκη

Κανελλοπούλου -Μπότη, Μ., 2020,*Αρχείο και Δίκαιο*, Αθήνα: Νομική Βιβλιοθήκη

Καρκατζούνης, Β., 2019,*Προστασία δεδομένων ήδη από το σχεδιασμό (bydesign) και εξ' ορισμού (bydefault), Μια πρώτη προσέγγιση του άρθρου 25 ΓΚΠΔ* ,TechCrime τευχ.8, διαθέσιμο σε

http://www.crimetimes.gr/%CF%80%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83% CE%AF%CE%B1-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD- %CE%AE%CE%B4%CE%B7-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF-%CF%83%CF%87%CE%B5%CE%B4%CE%B9%CE%B1/ (τελευταία πρόσβαση 31/10/2024)

Λαζαράκος Γ., επ. Βλαχόπουλος, Σ., 2017, *Θεμελιώδη Δικαιώματα*, Αθήνα: Νομική Βιβλιοθήκη

Λουκάς, Ν., 2017, *Τεχνικά μέτρα του Γενικού Κανονισμού για την προστασία Δεδομένων (GDPR) –Κρυπτογράφηση και Ψευδωνυμοποίηση*, ΣΥΝ 123/2017, σελ. 46-48

Λουκάς, Ν., *2019, Γενικός Κανονισμός για την Προστασία Δεδομένων– Πρακτικά ζητήματα σχετικά με την προστασία των προσωπικών δεδομένων (από τον σχεδιασμό)*, ΔiΜΕΕ, 1/2019, σελ.46-51

Λουκάς, Ν., 2018, *Προστασία των Δεδομένων από τον Σχεδιασμό στον Γενικό Κανονισμό για την Προστασία Δεδομένων*, ΣΥΝ, 5/2018, σελ. 38 - 41

Βόρρας Ά., επ. Μήτρου Λ., 2023,*Μπορεί ο Αλγόριθμος να είναι ηθικός, να είναι δίκαιος, να είναι διαφανής, να δικάζει και να διοικεί*, Πανεπιστημιακές Εκδόσεις Κρήτης

Μήτρου Λ., επ. Τολιόπουλος Ν., 2024, *Η Ιδιωτικότητα στην ψηφιακή εποχή*, Αθήνα: Νομική Βιβλιοθήκη

Μήτρου, Λ., 2013, *Privacy by Design. Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων*, ΔiΜΕΕ 1/2013, Τεύχος 1/2013, σελ.14-25

Μήτρου, Λ.και Καρυδά Μ., 2012,*"EU΄s Data Protection Reform and the right to be forgotten - A legal response to a technological challenge?*, International Conference of Information Law and Ethics, σελ.1-23 διαθέσιμο σε

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2165245 τελευταία πρόσβαση 31/10/2024)

Παλαιολόγου, Ε. και Πλιαβέσης, Γ., 2020, *Παρουσίαση – Σχολιασμός, Ν. 4624/201*

9 digesta μελέτες, σελ.1-7 διαθέσιμο σε http://digestaonline.gr/pdfs/Digesta%202020/gdpr.pdf (τελευταία πρόσβαση 20/9/2024)

Παναγοπούλου, Φ., επ. Βλαχόπουλος Σπ., Κοντιάδης Ξ., Τασόπουλος Γ., 2023, *Σύνταγμα – Ερμηνεία κατ' άρθρο, Άρθρο 9Α*, διαθέσιμο σε https://www.syntagmawatch.gr/wp-content/uploads/2023/02/%CE%86%CF%81%CE%B8%CF%81%CE%BF-9%CE%91-%CE%9C%CE%95-COVER-1.pdf (τελευταία πρόσβαση 29/10/2024)

Παναγοπούλου Κουτνατζή, Φ., 2012, *Κοινωνικά δίκτυα και προσωπικότητα-Ι,*ΔiΜΕΕ, 2/2012, 181-195

Παναγοπούλου Κουτνάτζη,Φ., 2019, *Συνταγματική Θεώρηση του νόμου περί προστασίας δεδομένων (Ν. 4624/2019)*, τ.3/2019,ΔiΜΕΕ, σελ. 328-337

Παναγοπούλου, Φ., επ. Βλαχόπουλος Σπ., Κοντιάδης Ξ., Τασόπουλος Γ., 2024, *Σύνταγμα – Ερμηνεία κατ' άρθρο*, Αθήνα : Νομική Βιβλιοθήκη

Παπακωνσταντίνου, Σ., 2024, *ΑΠΔΠΧ 10/2024 Επιβολή προστίμου 2.995.140 στα ΕΛΤΑ για την παραβίαση των αρχών της ακεραιότητας και της εμπιστευτικότητας και της ασφάλειας επεξεργασίας δεδομένων*, e-ΠΟΛΙΤΕΙΑ 11/2024, σελ. 453-463 , διαθέσιμο σε https://www.epoliteia.gr/wpcontent/uploads/2024/07/%CE%A3%CE%A7%CE%9F%CE%9B%CE%99%CE%912.pdf (τελευταία πρόσβαση 20/9/2024)

Παπαδημητρίου, Θ.,επ. Β. Γ. Τζέμος, 2015, *Ο Χάρτης Θεμελιωδών Δικαιωμάτων Της ΕΕ, Ερμηνεία Κατ' Άρθρο,* Αθήνα: Νομική Βιβλιοθήκη

Πισκοπάνη, Ά-Μ., 2009, «*Η προστασία της ιδιωτικότητας των χρηστών του Facebook*», ΔiΜΕΕ, 3/2009, σελ. 338 – 353

Πλιαβέσης, Γ., 2019, *Η Προστασία Των Προσωπικών Δεδομένων Στη Σχέση Τράπεζας – Πελάτη*, Αθήνα: Νομική Βιβλιοθήκη

Σταθόπουλος, Μ., 2004, *Επιτομή Γενικού Ενοχικού Δικαίου*, , Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη

Στεργιάδης, Α., 2020, *Περί του Γενικού Κανονισμού Προστασίας Δεδομένων και άλλων (καινών) δαιμονίων*, ΔΕΕ 5/2020, σελ. 518-525

Συμεωνίδου, Χ., 2017, *Ο ρόλος του Data Protection Officer και η χρήση της ασφάλισης cyberinsurance – Γενικός Κανονισμός Προστασίας Δεδομένων* (GDPR), ΣΥΝήγορος, 121/2017, σελ.1-5

Τιντζογλίδου, Ν., 2022, *Οδηγός Εφαρμογής GDPR*, Αθήνα: Νομική Βιβλιοθήκη

Τζώρτζη, Β., 2017, *Προστασία δεδομένων προσωπικού χαρακτήρα: οι σημαντικότερες αλλαγές από τον Γενικό Κανονισμό*, Εφαρμογές Δημοσίου Δικαίου, Αθήνα: Νομική Βιβλιοθήκη

Φαραντούρης, Ν., επ. Χριστιανός Β., ,2012,*Συνθήκη ΕΕ & ΣΛΕΕ (Κατ' άρθρο ερμηνεία)*, Αθήνα: Νομική Βιβλιοθήκη

Χριστοδούλου, Κ., 2020, *Δίκαιο Προσωπικών Δεδομένων*, Αθήνα: Νομική Βιβλιοθήκη,

<u>Νομοθεσία</u>

Άρθρο 9 Σ

Άρθρο $9^{α}$ Σ

άρθρο 93 Συντ.

Άρθρο 16 ΣΛΕΕ

Άρθρο 8 ΕΣΔΑ

Άρθρο 7 ΧΘΔΕΕ

Άρθρο 8 ΧΘΔΕΕ

Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679 (ΕΕ)

Κανονισμός (ΕΕ) 2019/881

Κανονισμός 910/2014 (κανονισμός e-IDAS)

Κανονισμός 2024/1183

Ν. 3659/2008

Ν. 3471/2006

Νόμο 2774/1999

Ν. 3979/2011

Ν. 4624/2019

Ν.2472/1997

Οδηγία 2002/58/ΕΚ (οδηγία e-privacy)

Οδηγία 95/46/ΕΚ

Οδηγία 2016/680/ΕΕ

Πρόταση Κανονισμού e- Privacy

Σύμβαση 108 του Συμβουλίου της Ευρώπης του 1981

Νομολογία

Google Spain

ΑΠΔΠΧ 31/2019

ΑΠΔΠΧ 34/2019

ΑΠΔΠΧ 4/2022

ΑΠΔΠΧ 10/2024

Γνωμοδοτήσεις - Ανακοινώσεις

Agencia Española de Protección de Datos (AEPD), *Guide to Privacy by Design* ,pp.1-54 διαθέσιμο σε https://www.aepd.es/guides/guide-to-privacy-by-design.pdf (τελευταία πρόσβαση 21/1/2025)

European Data Protection Supervisor, *Opinion* 5/2018, *Preliminary Opinion on privacy by design*,pp.1-34, διαθέσιμη σε https://www.edps.europa.eu/sites/default/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (τελευταία πρόσβαση 21/1/2025)

Opinion of the European Data Protection Supervisor, on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 2011,«*A comprehensive approach on personal data protection in the European Union*»,pp.1-36διαθέσιμο σε https://www.edps.europa.eu/sites/default/files/publication/11-01-14_personal_data_protection_en.pdf (τελευταία πρόσβαση 30/10/2024)

European Data Protection Supervisor,2017, *Opinion 6/2017 "Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)"*, p.1-40, διαθέσιμο σε https://www.edps.europa.eu/sites/default/files/publication/17-04-24_eprivacy_en.pdf (τελευταία πρόσβαση 31/10/2024)

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), 2020, *Κατευθυντήριες γραμμές 4/2019 σύμφωνα με το άρθρο 25 Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού*, Έκδοση 2.0, διαθέσιμο σε https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_el.pdf(τελευταία πρόσβαση στις 16/10/2024)