ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΣΥΓΧΡΟΝΟ ΤΕΧΝΟΛΟΓΙΚΟ ΠΕΡΙΒΑΛΛΟΝ

Διπλωματική Εργασία

του

Βάιου Ντόκα

Θεσσαλονίκη, 06/2021

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΣΥΓΧΡΟΝΟ ΤΕΧΝΟΛΟΓΙΚΟ ΠΕΡΙΒΑΛΛΟΝ

Βάιος Ντόκας

Πτυχίο Νομικής, ΑΠΘ, 2008

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπουσα Καθηγήτρια: Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία

Επιβλέπων Καθηγητής: Μαυρίδης Ιωάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 22/6/2021

Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία	Μαυρίδης Ιωάννης	Φουληράς Παναγιώτης
.....	.....	.....

Βάιος Ντόκας

Περίληψη

Η προστασία των προσωπικών δεδομένων στα σύγχρονα πληροφοριακά συστήματα και στο διαδίκτυο καθίσταται όλο και πιο δύσκολη λόγω της χρήσης νέων τεχνολογιών ανάλυσης και επεξεργασίας δεδομένων αλλά και εξαιτίας της καθυστέρησης της νομοθεσίας να προσαρμοστεί στις νέες και συνεχώς εξελισσόμενες τεχνολογίες. Παρά τις προκλήσεις που εμφανίζονται όμως, καινοτόμες τεχνολογίες όπως η χρησιμοποίηση των δικτύων του blockchain αλλά και των σύγχρονων τεχνικών ανωνυμοποίησης και κρυπτογράφησης μπορούν, εφόσον εφαρμοστούν ορθά, να προσφέρουν λύσεις που αντιμετωπίζουν τις εμφανιζόμενες δυσκολίες και να αυξήσουν το επίπεδο προστασίας των προσωπικών δεδομένων.

Στην παρούσα εργασία αρχικά θα γίνει μια μελέτη του διεθνούς και ελληνικού νομοθετικού πλαισίου προστασίας των προσωπικών δεδομένων και θα αναλυθούν οι διεθνείς κανόνες ασφαλούς επεξεργασίας και διαβίβασης δεδομένων. Έπειτα, θα αναλυθούν οι βασικές έννοιες της ασφάλειας πληροφοριών όσον αφορά πληροφοριακά συστήματα και θα αναζητηθούν οι βέλτιστοι τρόποι ενίσχυσης της αρχής της διαφάνειας μέσω του ασφαλούς σχεδιασμού πληροφοριακών συστημάτων, πολιτικών χρήσης και ασφαλών εφαρμογών. Θα γίνει επίσης ανάλυση των τεχνικών μέτρων που προάγουν την ασφάλεια, την διαφάνεια και την ανωνυμία και χρησιμοποιούνται στην προστασία των προσωπικών δεδομένων. Τέλος θα αναλυθεί η τεχνολογία αλλά και οι προοπτικές χρήσης των σύγχρονων τεχνικών κρυπτογράφησης όπως και της τεχνολογίας blockchain και έξυπνων συμβολαίων ως τεχνικών για την διασφάλιση των αρχών της ακεραιότητας και της διαφάνειας.

Λέξεις Κλειδιά:

Προσωπικά δεδομένα, ιδιωτικότητα, νομοθεσία, ασφάλεια δεδομένων, ασφαλής σχεδιασμός πληροφοριακών συστημάτων, κρυπτογράφηση, ανωνυμοποίηση, ψευδωνυμοποίηση, blockchain, έξυπνα συμβόλαια.

Abstract

The protection of personal data in modern informational systems and the internet is becoming increasingly challenging due to the implementation of new technologies of analysis and process of data as well as the procrastination of the legislation to adapt to these new and constantly evolving technologies. Despite the challenges emerging, innovative technologies such as the use of blockchain networks as well as modern anonymization and encryption techniques, can provide solutions, if properly applied, at overcoming the emerging difficulties and raise the level of protection of personal data.

In the present paper, there will be a study of the international and Greek legislation framework of protection of personal data and there will be an analysis of the international rules of safe process and transfer of data. Consequently, the basic principles of information security in the scope of information systems will be analyzed and there will be a search for the optimal ways to strengthen the principle of transparency through secure design of information systems, policies and secure applications. There will also be an analysis of technical measures that promote security, transparency and anonymity and can be applied in the protection of personal data. Finally, modern encryption technologies, blockchain and smart contracts will be examined for their potential use as tools for augmenting integrity and transparency.

Keywords:

Personal data, privacy, legislation, data security, data protection by design, encryption, anonymisation, pseudonymisation, blockchain, smart contracts.

Πρόλογος – Ευχαριστίες

Το μεταπτυχιακό «Δίκαιο και Πληροφορική» ήταν μια μοναδική εκπαιδευτική εμπειρία για μένα και το σημείο όπου ενώθηκαν οι δύο επιστήμες της ζωής μου, η νομική και η πληροφορική, σαν δύο κομμάτια του παζλ, ανοίγοντάς μου νέους ορίζοντες.

Θα ήθελα να ευχαριστήσω θερμά τους καθηγητές μου και επιβλέποντες καθηγητές της παρούσας εργασίας, κα Ευγενία Αλεξανδροπούλου και κ. Ιωάννη Μαυρίδη, οι οποίοι με τις γνώσεις τους, την άψογη καθοδήγηση τους αλλά και την εμπιστοσύνη τους στο πρόσωπό μου, με βοήθησαν να ολοκληρώσω τη διπλωματική μου εργασία.

Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένειά μου, την σύζυγό μου, τον γιο μου και την κόρη μου, για την αμέριστη υπομονή και στήριξη που μου επέδειξαν, αφού χωρίς αυτούς δεν θα ήταν δυνατό αυτό το υπέροχο «ταξίδι» στην γνώση.

Περιεχόμενα

Συντομογραφίες

1. Ελληνικές Συντομογραφίες

ΑΠΔΠΧ	Ελληνική Αρχή Προστασίας των Προσωπικών Δεδομένων
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Δεδομένων
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΔΕΚ	Δικαστήριο των Ευρωπαϊκών Κοινοτήτων
ΔΕΥ	Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων
ΕΑΠΔ	Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων
ΕΔΑΔ	Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΕΚ	Ευρωπαϊκό Κοινοβούλιο
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΝΔ	Νομοθετικό Διάταγμα
ΟΗΕ	Οργανισμός Ηνωμένων Εθνών
ΟΔΔΑ	Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα
ΟΟΣΑ	Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης
Σ	Σύνταγμα
ΣτΕ	Συμβούλιο της Επικρατείας
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
ΤΠΕ	Τεχνολογίες της Πληροφορικής και της Επικοινωνίας
ΤΣΡ	Τυποποιημένες Συμβατικές Ρήτρες

2. Ξενόγλωσσες Συντομογραφίες

AES	Advanced Encryption Standard
Bit	Binary Digit
CCPA	California Consumer Privacy Act
CNIL	Commission Nationale de l'Informatique et des Libertés
CobIT	Control Objectives for Information Technology
DES	Data Encryption Standard

DLT	Distributed Ledger Technology
DPbDD	Data Protection by Design and by Default
DPIA	Data Protection Impact Assessment
HTTPS	Hypertext Transfer Protocol Secure
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
EE L	Official Journal of the European Union L
ENISA	EUROPEAN UNION AGENCY FOR CYBERSECURITY
EPPO	European Public Prosecutor's Office
EuroPriSe	European Privacy Seal
Europol	European Union’s law enforcement agency
HIPAA	Health Insurance Portability and Accountability Act
ICO	Initial Coin Offering
IPO	Initial Public Offering
IoT	Internet of Things
ISO/IEC	International Organization for Standardization (ISO) and the International Electrotechnical Commission
NIST/SP	National Institute of Standards and Technology / Special Publication
OECD	Organisation for Economic Co-operation and Development
PETs	Privacy Enhancing Technologies
RSA	Rivest–Shamir–Adleman (cryptosystem)
SaaS	Software as a service
WP29	Working Party of Article 29

1 ΕΙΣΑΓΩΓΗ

1.1 Το πρόβλημα της ασφάλειας στα προσωπικά δεδομένα

Οι προκλήσεις στην προστασία των προσωπικών δεδομένων -με την διάδοση της χρήσης των νέων τεχνολογιών- αυξάνονται με εκθετικό βαθμό. Η προσπάθεια προστασίας της ιδιωτικότητας των υποκειμένων των δεδομένων καθίσταται δυσκολότερη λόγω της χρήσης νέων τεχνολογιών στον τομέα της επεξεργασίας των δεδομένων, που καθιστούν ευκολότερη την αυτοματοποιημένη κατάρτιση προφίλ, αλλά και των δυσκολιών ενσωμάτωσης τεχνικών ανωνυμοποίησης και ψευδωνυμοποίησης. Πρόβλημα που έχει ενταθεί και από τις συνέπειες της πανδημίας του covid-19 και του πρόσφατου αναγκαστικού περιορισμού των ατομικών δικαιωμάτων βάσει της αρχής της αναλογικότητας. Δυσκολίες εμφανίζονται επίσης, στην άσκηση των δικαιωμάτων των υποκειμένων και στην εύρεση κατάλληλων και αποδοτικών μέτρων λήψης συναίνεσης αλλά και ασφαλούς διατήρησης και διαβίβασης των δεδομένων τους, από οργανισμούς που τα διαχειρίζονται.

Από την πλευρά των οργανισμών, οι δυσκολίες στην ασφάλεια των προσωπικών δεδομένων εντοπίζονται σε θέματα ενσωμάτωσης των απαιτήσεων του νόμου όσον αφορά την λήψη τεχνικών και οργανωτικών μέτρων, την τήρηση προτύπων αλλά και την ενσωμάτωση των αρχών του ασφαλούς σχεδιασμού και της ασφάλειας εξ ορισμού στα πληροφοριακά τους συστήματα. Η εφαρμογή των τεχνικών μέτρων με την χρήση νέων τεχνολογιών, απαιτεί αποδοτική ενσωμάτωση των σχεδιαζόμενων μέτρων στην διατήρηση και επεξεργασία των δεδομένων μέσω της χρήσης των τεχνικών της κρυπτογραφίας της ανωνυμοποίησης και της ψευδωνυμοποίησης, όταν απαιτείται, με τρόπο που να είναι εφαρμόσιμο τεχνολογικά, βιώσιμο οικονομικά για τον οργανισμό αλλά και να ανταποκρίνεται στο επίπεδο ασφαλείας που απαιτείται για την κάθε περίπτωση.

Πολλά είναι επίσης, τα περιστατικά απώλειας εμπιστευτικότητας λόγω κυβερνοεπιθέσεων ή οι περιπτώσεις ηλεκτρονικής απάτης όπως και τα προβλήματα ασφάλειας σε προσπάθειες ενσωμάτωσης νέων τεχνολογιών στο σχεδιασμό πληροφοριακών συστημάτων με σκοπό την εξασφάλιση της διαφάνειας. Πολλά από αυτά τα προβλήματα θα μπορούσαν να αντιμετωπιστούν με την εφαρμογή της τεχνολογίας του blockchain, των έξυπνων συμβολαίων αλλά και της διενέργειας των συναλλαγών με τη χρήση ψηφιακών νομισμάτων.

1.2 Σκοπός – Στόχοι

Η έναρξη ισχύος του Γενικού Κανονισμού για την Προστασία Δεδομένων (2016/679) το 2018 δημιούργησε ένα αυστηρότερο και ομοιογενές θεσμικό πλαίσιο σχετικά με την επεξεργασία και την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ε.Ε. και αποτέλεσε το σημείο καμπής που έθεσε σε δοκιμασία τις πολιτικές διαχείρισης δεδομένων, τα τεχνικά και οργανωτικά μέτρα προστασίας αλλά και τις απαιτήσεις για αναλύσεις αντικτύπου των παραβιάσεων. Σκοπός της παρούσας μελέτης είναι να εντοπιστεί το συνολικό νομοθετικό πλαίσιο και οι κανόνες που διέπουν την προστασία των προσωπικών δεδομένων στο Ευρωπαϊκό νομοθετικό σύστημα αλλά και τον τρόπο που θα μπορούσαν αυτοί να εφαρμοστούν στην πράξη με τη χρήση νέων τεχνολογιών. Αφού αναλυθούν τα οριζόμενα περί ασφάλειας δεδομένων προσωπικού χαρακτήρα στον ΓΚΠΔ, θα αναζητηθούν οι βέλτιστοι τρόποι προστασίας προσωπικών δεδομένων μέσω της βελτίωσης της πλαισίου παροχής ασφάλειας στα δεδομένα, την τήρηση της αρχής της διαφάνειας και την χρήση ορθών πολιτικών και ασφαλών πληροφοριακών συστημάτων εκ του σχεδιασμού. Θα αναλυθούν επίσης, οι αρχές του ασφαλούς σχεδιασμού, της προστασίας εξ ορισμού και οι τρόποι τήρησης των αρχών του ΓΚΠΔ, ώστε να μπορεί ένα πληροφοριακό σύστημα να πληροί τις απαιτήσεις του νόμου. Στους στόχους της μελέτης είναι και η εύρεση των κατάλληλων τεχνικών μέτρων και η μελέτη της δυνατότητας ενσωμάτωσης νέων τεχνολογιών, όπως αυτές του blockchain και της ανωνυμοποίησης με χρήση κρυπτογραφίας, που μπορούν να εκπληρώσουν την ανάγκη λήψεως τεχνικών μέτρων που ορίζει αλλά δεν εξειδικεύει ο Κανονισμός.

2 ΔΙΑΡΘΡΩΣΗ ΜΕΛΕΤΗΣ

Η παρούσα μελέτη θα παραθέσει πρώτα το νομοθετικό πλαίσιο προστασίας των προσωπικών δεδομένων και έπειτα θα αναλύσει τον τρόπο και τα μέσα με τα οποία μπορεί να επιτευχθεί αυτή η προστασία.

Στο 3ο κεφάλαιο θα γίνει μια συνολική επισκόπηση του νομοθετικού πλαισίου, όπως αυτό ισχύει από το πρωτογενές και παράγωγο δίκαιο της Ευρώπης μέχρι και τον τελευταίο Ελληνικό Νόμο 4624/2019.

Στο 4ο κεφάλαιο θα αναλυθούν οι κανόνες ασφαλούς επεξεργασίας, όπως αυτό καθιερώνεται από το άρθρο 32 επ. του ΓΚΠΔ και θα αναλυθεί η υποχρέωση διασφάλισης ασφαλούς επεξεργασίας, οι τρόποι που μπορεί να διασφαλιστεί η ασφάλεια αυτή μέσω διεθνών προτύπων, αλλά και βασικές έννοιες της ασφάλειας όπως η εμπιστευτικότητα και η ακεραιότητα. Θα εκτεθεί επίσης η υποχρέωση γνωστοποίησης, τα κριτήρια αξιολόγησης του κινδύνου και τι ισχύει σε περίπτωση που τα δεδομένα είναι ανωνυμοποιημένα.

Στο 5ο κεφάλαιο θα αναλυθούν θέματα ασφάλειας πληροφοριών και οι τρόποι ασφαλούς σχεδιασμού πληροφοριακών συστημάτων. Επιπρόσθετα, θα αναζητηθούν οι τρόποι ενίσχυσης της αρχής της διαφάνειας, μέσω της εκτίμησης αντικτύπου και τήρησης πιστοποιήσεων ασφαλείας στην επεξεργασία και διαβίβαση δεδομένων. Στον σχεδιασμό πληροφοριακών συστημάτων θα αναλυθούν οι απαιτήσεις κατά την συλλογή, την διατήρηση και ανάλυση των δεδομένων, την τήρηση των αρχών κατά την επεξεργασία, την ασφαλή διαγραφή και προβλήματα που συνήθως προκύπτουν στον τομέα αυτό.

Στο 6ο κεφάλαιο θα γίνει μια επαφή με την έννοια της κρυπτογραφίας, τις διακρίσεις αυτής ως συμμετρική και ασύμμετρη, πώς μπορεί αυτή να ενισχύσει την ασφάλεια και θα παρατεθούν ορισμένα εργαλεία ενίσχυσης της ακεραιότητας και της αυθεντικοποίησης. Θα μελετηθούν επίσης, όλοι οι μέθοδοι απόκρυψης της ταυτότητας, με ανάλυση τεχνικών της ανωνυμοποίησης όπως η τυχαιοποίηση και η γενίκευση γνωρισμάτων, η τεχνική της ψευδωνυμοποίησης, η δυνατότητα χρήσης έξυπνων συμβολαίων προς αυτό το σκοπό και τα προβλήματα που μπορεί να προκύψουν στις τεχνικές αυτές με την επαναταυτοποίηση των υποκειμένων.

Τέλος στο 7ο κεφάλαιο θα γίνει μια ανάλυση της τεχνολογίας του blockchain, με τις διαφοροποιήσεις του, τους τρόπους λειτουργίας του αλλά και του bitcoin που αποτελεί την γνωστότερη εφαρμογή της τεχνολογίας αυτής. Θα αναλυθούν επίσης, οι νομικές

πτυχές του blockchain και των έξυπνων συμβολαίων αλλά και η νομοθετική αντιμετώπισή τους στην Ευρώπη και της Ελλάδα.

3 ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Τα προσωπικά δεδομένα διαδραματίζουν σημαντικό ρόλο στη σύγχρονη ζωή ιδιαιτέρως μετά την ανάπτυξη του διαδικτύου που σηματοδότησε μία νέα εποχή για την επικοινωνία. Η προστασία των προσωπικών δεδομένων σε διεθνές, κοινοτικό και εθνικό επίπεδο καταδεικνύει την σπουδαιότητα αυτού του εννόμου αγαθού. Βάσει του δικαίου της ΕΕ, η προστασία δεδομένων αναγνωρίζεται ως διακριτό θεμελιώδες δικαίωμα. Προβλέπεται στο άρθρο 16 της Συνθήκης για τη λειτουργία της ΕΕ καθώς και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ και πλέον προστατεύεται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων, ο οποίος τέθηκε σε εφαρμογή τον Μάιο του 2018.

3.1 Κύριες διεθνείς πράξεις για την προστασία των δεδομένων

3.1.1 Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα (ΟΔΔΑ)

Σε διεθνές επίπεδο η προστασία των προσωπικών δεδομένων κατοχυρώνεται αρχικά από την Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα[1]. Παρότι η Σύμβαση δεν προβλέπει μέτρα προστασίας των ατόμων σε περίπτωση παραβίασης των διατάξεών της, η διακήρυξη που υιοθετήθηκε από τα τότε κράτη των Ηνωμένων Εθνών, επίδρασε σημαντικά στη θέσπιση πράξεων για τα ανθρώπινα δικαιώματα στην Ευρώπη.

3.1.2 Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (ICCPR)

Ο Οργανισμός Ηνωμένων Εθνών (ΟΗΕ) έχει εκδώσει το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (ICCPR) το οποίο τέθηκε σε ισχύ το 1976. Διακηρύσσει ότι ουδείς υποβάλλεται σε αυθαίρετες ή παράνομες επεμβάσεις στην ιδιωτική ζωή, στην κατοικία ή στην αλληλογραφία του, ούτε σε παράνομες προσβολές της τιμής και της υπόληψής του. Το ICCPR είναι διεθνής συνθήκη η οποία δεσμεύει τα 169 συμβαλλόμενα μέρη της, ώστε να σέβονται και να διασφαλίζουν την άσκηση των

[1] Βλ. Οργανισμό Ηνωμένων Εθνών (ΟΗΕ), Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα (αρ.12), 10 Δεκεμβρίου 1948 όπου: "Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους" (http://www.un.org/en/documents/udhr/index.shtml).

ατομικών δικαιωμάτων των φυσικών προσώπων, συμπεριλαμβανομένου του δικαιώματος στην ιδιωτική ζωή. Από το 2013, ο Οργανισμός Ηνωμένων Εθνών έχει εκδώσει δύο αποφάσεις σχετικά με ζητήματα της ιδιωτικής ζωής με τίτλο «το δικαίωμα στην ιδιωτική ζωή στην ψηφιακή εποχή»[2] ως απάντηση στην ανάπτυξη νέων τεχνολογιών και στις αποκαλύψεις περί μαζικής παρακολούθησης που διενεργήθηκε σε ορισμένα κράτη (αποκαλύψεις Snowden). Σε αυτές καταδικάζεται έντονα η μαζική παρακολούθηση και τονίζεται ο αντίκτυπος που μπορεί να έχει αυτού του είδους η παρακολούθηση στα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και στην ελευθερία έκφρασης, καθώς και στη λειτουργία μιας σφύζουσας και δημοκρατικής κοινωνίας. Παρότι δεν είναι νομικά δεσμευτικές, οι αποφάσεις αυτές πυροδότησαν ευρύ διεθνή πολιτικό διάλογο υψηλού επιπέδου σχετικά με την ιδιωτική ζωή, τις νέες τεχνολογίες και την παρακολούθηση. Οδήγησαν επίσης στον διορισμό Ειδικού Εισηγητή για το δικαίωμα στην ιδιωτικότητα, με εντολή την προαγωγή και την προστασία του δικαιώματος αυτού. Στα ειδικά καθήκοντα του εισηγητή περιλαμβάνονται η συλλογή πληροφοριών σχετικά με τις εθνικές πρακτικές και εμπειρίες σε σχέση με την ιδιωτική ζωή και οι προκλήσεις που απορρέουν από τις νέες τεχνολογίες, η ανταλλαγή και η προώθηση βέλτιστων πρακτικών, καθώς και ο προσδιορισμός δυνητικών εμποδίων.

3.1.3 Οι Κατευθυντήριες Αρχές του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ)

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) είναι ένας διεθνής οργανισμός ο οποίος στοχεύει στην προώθηση πολιτικών με σκοπό την οικονομική ανάπτυξη. Ο Οργανισμός αυτός σχετίστηκε με την προστασία προσωπικών δεδομένων εκδίδοντας, το 1980, τις Κατευθυντήριες Αρχές για την «προστασία της ιδιωτικότητας και τη διασυνοριακή αποστολή προσωπικών δεδομένων». Οι Οδηγίες αυτές του ΟΟΣΑ ήταν και παραμένουν μη δεσμευτικές. Το διεθνές αυτό κείμενο περιλαμβάνει αρχές, όπως: την αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων, την αρχή της ποιότητας των δεδομένων, την αρχή της διαφάνειας, την αρχή της συμμετοχής του ατόμου, την αρχή της ευθύνης, την αρχή του προσδιορισμού του σκοπού κ.α.[3] Σήμερα,

[2] Βλ. ΟΗΕ, Γενική Συνέλευση, Resolution on the right to privacy in the digital age, A/RES/68/167, Νέα Υόρκη, 18 Δεκεμβρίου 2013· και ΟΗΕ, Γενική Συνέλευση, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, Νέα Υόρκη, 19 Νοεμβρίου 2014.

[3] Διατίθεται ηλεκτρονικά:

τις Οδηγίες τις έχουν υιοθετήσει συνολικά τριάντα τέσσερις χώρες. Οι ανωτέρω Οδηγίες και η έντονη διεθνής επιρροή, τους άνοιξαν το δρόμο για το Συμβούλιο της Ευρώπης και τη Σύμβαση 108.

3.2 Θεμελιώδες Ευρωπαϊκό Δίκαιο

3.2.1 Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)

Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ)[4] τέθηκε σε ισχύ το 1953 και αποτελεί διεθνή υποχρέωση των κρατών μελών του Συμβουλίου της Ευρώπης που σήμερα ανέρχονται σε σαράντα επτά (47). Όλα τα κράτη μέλη του Συμβουλίου έχουν ενσωματώσει την ΕΣΔΑ στο εθνικό τους δίκαιο και υποχρεούνται να σέβονται το περιεχόμενο των διατάξεών της. Η χώρα μας έχει μεταφέρει την ΕΣΔΑ στο εθνικό μας δίκαιο με το ΝΔ 53/1974 που έχει αυξημένη τυπική ισχύ[5] σύμφωνα με το Σύνταγμά μας[6]. Το άρθρο 8 της ΕΣΔΑ με τίτλο «Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής» κατοχυρώνει την ιδιωτική ζωή και επικοινωνία και μεταξύ άλλων, το δικαίωμα στην προστασία των προσωπικών δεδομένων. Εγγυάται το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και ορίζει τις προϋποθέσεις υπό τις οποίες μπορεί να θεωρηθεί αποδεκτή η κρατική επέμβαση στο δικαίωμα αυτό[7]. Σύμφωνα με την νομολογία του ΕΔΑΔ, το αρ.8 της ΕΣΔΑ υποχρεώνει τα κράτη όχι μόνο να απέχουν από κάθε αυθαίρετη επέμβαση επί του δικαιώματος αυτού, αλλά και να λαμβάνουν τα απαραίτητα μέτρα για την ουσιαστική διασφάλιση του σεβασμού της ιδιωτικής και οικογενειακής ζωής[8].

---

http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflows ofpersonaldata.htm (τελευταία πρόσβαση 12-2-2021)

[4] Διατίθεται και ηλεκτρονικά στον επίσημο ιστότοπο του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων: https://www.echr.coe.int/documents/convention_ell.pdf (τελευταία πρόσβαση 12-2-2021)

[5] Βλ. Εμμανουήλ Ρούκουνα, Διεθνής Προστασία των Ανθρωπίνων Δικαιωμάτων (Αθήνα: Εστία, 1995), σελ. 106

[6] Βλ. αρ.28§1, εδ.α' Σ όπου: "Οι γενικά παραδεγμένοι κανόνες του διεθνούς δικαίου, καθώς και οι διεθνείς συμβάσεις, από την επικύρωσή τους με νόμο και τη θέση τους σε ισχύ σύμφωνα με τους όρους καθεμιάς, αποτελούν αναπόσπαστο μέρος του εσωτερικού ελληνικού δικαίου και υπερισχύουν από κάθε άλλη αντίθετη διάταξη νόμου"

[7] Βλ. ΕΣΔΑ, αρ.8 "Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής"

[8] Βλ. ΕΔΑΔ, 13.06.1979, Marckx v.Belgium (αριθμ.6833/74), §31 όπου αναφέρεται χαρακτηριστικά: "…Article 8 signifies firstly that the State cannot interfere with the exercise of that right otherwise than in accordance with the strict conditions set out in ar.8§2...the object of the Article is "essentially" that of protecting the individual against arbitrary interference by the public authorities…it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be

3.2.2 Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Οι αρχικές συνθήκες των Ευρωπαϊκών Κοινοτήτων δεν είχαν καμία πρόβλεψη για τα ανθρώπινα δικαιώματα ή στην προστασία τους. Οι πολιτικές όμως της Ευρωπαϊκής Ένωσης στα ανθρώπινα δικαιώματα, το 2000 την οδήγησαν στην πανηγυρική διακήρυξη του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Ο Χάρτης περιέχει μια πληθώρα ατομικών, πολιτικών, κοινωνικών και οικονομικών δικαιωμάτων υπέρ των ευρωπαίων πολιτών που αφορούν την αξιοπρέπεια, τις ελευθερίες, την ισότητα, την αλληλεγγύη, τα δικαιώματα των πολιτών και τη δικαιοσύνη[9].

Τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ αναγνωρίζουν τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα ως στενά συνδεδεμένα, αλλά ξεχωριστά, θεμελιώδη δικαιώματα.

3.2.3 Επικαιροποιημένη Σύμβαση 108 του Συμβουλίου της Ευρώπης

Η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων (Σύμβαση 108) του Συμβουλίου της Ευρώπης της 28ης Ιανουαρίου 1981 είναι το μόνο νομικά δεσμευτικό διεθνές σύμφωνο που αφορά ειδικά την προστασία των προσωπικών δεδομένων[10]. Σκοπός της είναι η διασφάλιση για κάθε φυσικό πρόσωπο «του σεβασμού των δικαιωμάτων του και των θεμελιωδών ελευθεριών του, και ιδίως του δικαιώματός του στην ιδιωτική ζωή, έναντι της αυτοματοποιημένης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα».

Το δεσμευτικό αλλά και διεθνές αυτό κείμενο, υποχρεώνει τα κράτη που το κύρωσαν σε θετική δράση και θέσπιση μέτρων για την προστασία των προσωπικών δεδομένων των πολιτών και κατ' επέκταση για την διασφάλιση των ατομικών δικαιωμάτων τους[11].

---

positive obligations…". Ομοίως, ΕΔΑΔ, 9.10.1979, Airey v. Ireland (αριθμ.6289/73), §32 αλλά και οι πιο πρόσφατες αποφάσεις: ΕΔΑΔ, 17.07.2008, I. v. Finland (αριθμ.20511/03), §36 και ΕΔΑΔ, 2.12.2008, K.U. v. Finland (αριθμ.2872/02), §42, §49

[9] Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, Εκδόσεις Νομική Βιβλιοθήκη, Θεσσαλονίκη, 2016, σελ. 210 επ. και Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, https://fra.europa.eu/el/publication/2020/egheiridio-shetika-me-tin-eyropaiki-nomothesia-gia-tin-prostasia-ton-prosopikon, 2018, (τελευταία πρόσβαση 31 Ιανουαρίου 2021) σελ.35 επ.

[10] Βλ. Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδ ομένων, Συμβούλιο της Ευρώπης, CETS αριθμ.108. 1981

[11] Βλ. Ειρηνικός Πλατής, Προσωπικά δεδομένα-Προστασία GDPR, Εκδόσεις Παπαδόπουλος, 2018, σελ. 26

Το 2001, με το πρόσθετο πρωτόκολλο στη Σύμβαση 108, υιοθετήθηκαν διατάξεις σχετικά με τη διασυνοριακή ροή δεδομένων προς μη συμβαλλόμενα μέρη, τις αποκαλούμενες «τρίτες χώρες», και σχετικά με την υποχρεωτική σύσταση εθνικών εποπτικών αρχών προστασίας των δεδομένων[12]. Το πρωτόκολλο για την τροποποίηση της Σύμβασης[13] της 17-18 Μαΐου 2018, αποσκοπεί στη διεύρυνση του πεδίου εφαρμογής της, στην αύξηση του επιπέδου προστασίας των δεδομένων και στη βελτίωση της αποτελεσματικότητάς της.

3.3 Ευρωπαϊκό Δίκαιο για την προστασία των προσωπικών δεδομένων

Εκτός από το πρωτογενές δίκαιο των Συνθηκών, το Ευρωπαϊκό δίκαιο περιλαμβάνει και τους κανόνες του δευτερογενούς ή παραγώγου δικαίου, δηλαδή αυτούς που θεσπίζουν τα όργανα της Ένωσης. Οι κανόνες αυτοί περιλαμβάνονται στις τρεις βασικές κατηγορίες πράξεων που προβλέπει το άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ). Πρόκειται για τους κανονισμούς, τις οδηγίες και τις αποφάσεις.

Ο Κανονισμός έχει γενική ισχύ, είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος, χωρίς δηλαδή τη μεσολάβηση εθνικής πράξης μεταφοράς των ρυθμίσεών του στο εθνικό δίκαιο. Πάντως, για την εφαρμογή ορισμένων διατάξεων κανονισμού ενδέχεται να είναι απαραίτητη η λήψη μέτρων εφαρμογής. Κατά πάγια νομολογία, τα κράτη μέλη δύνανται να θεσπίζουν μέτρα εφαρμογής ενός κανονισμού, εφόσον δεν παρακωλύουν την άμεση εφαρμογή του, δεν αποκρύπτουν την κοινοτική του φύση και διευκρινίζουν ότι πρόκειται για άσκηση της διακριτικής ευχέρειας την οποία τους παρέχει ο ίδιος ο Κανονισμός, χωρίς ωστόσο να γίνεται υπέρβαση των ορίων που θέτουν οι διατάξεις του ΔΕΚ της 14.10.2004[14].

---

[12] Βλ. ΣτΕ, Πρόσθετο πρωτόκολλο στη Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, σχετικά με τις εποπτικές αρχές και τις διασυνοριακές ροές δεδομένων, CETS αριθ. 181, 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181 και Βλ. Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, https://fra.europa.eu/el/publication/2020/egheiridio-shetika-me-tin-eyropaiki-nomothesia-gia-tin-prostasia-ton-prosopikon, 2018, (τελευταία πρόσβαση 31 Ιανουρίου 2021) σελ.29 και Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, Εκδόσεις Νομική Βιβλιοθήκη, Θεσσαλονίκη, 2016, σελ. 201

[13] Ηλεκτρονικά στον επίσημο ιστότοπο του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e (τελευταία πρόσβαση 12-2-2021)

[14] Βλ. C-113/02, Επιτροπή κατά Κάτω Χωρών, Συλλογή 2004, σ. I-9707, σκέψη 16. Βλ. και ΣτΕ ΠΕ 89/2007

Οι Οδηγίες αποτελούν ιδιότυπη πηγή του ευρωπαϊκού δικαίου, οι οποίες δεσμεύουν μεν κάθε κράτος μέλος ως προς το επιδιωκόμενο αποτέλεσμα, αφήνουν δε την επιλογή του τύπου και των μέσων στην αρμοδιότητα των εθνικών αρχών. Οι οδηγίες δεν έχουν συνεπώς άμεση ισχύ και είναι αναγκαία η έκδοση πράξης μεταφοράς τους στο εθνικό δίκαιο (εφαρμοστικούς νόμους).

3.3.1 Γενικός Κανονισμός για την Προστασία Δεδομένων (2016/679)

Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), τέθηκε σε ισχύ τον Μάιο του 2018[15]. Οι κανόνες αποσκοπούν στην προστασία όλων των πολιτών της ΕΕ από τις παραβιάσεις της ιδιωτικής ζωής και των δεδομένων σε έναν κόσμο που βασίζεται όλο και περισσότερο σε δεδομένα, ενώ παράλληλα δημιουργούν ένα σαφέστερο και συνεκτικότερο πλαίσιο για τις επιχειρήσεις. Τα δικαιώματα για τους πολίτες περιλαμβάνουν τη σαφή και επιβεβαιωμένη συγκατάθεσή τους για την επεξεργασία των δεδομένων τους και το δικαίωμα να λαμβάνουν σχετικές σαφείς και κατανοητές πληροφορίες, το δικαίωμα στη λήθη, το δικαίωμα στην διαγραφή των δεδομένων του κάθε πολίτη, το δικαίωμα διαβίβασης δεδομένων σε άλλον πάροχο υπηρεσιών (λ.χ. κατά τη μετάβαση από ένα πάροχο τηλεπικοινωνιών σε άλλο) και το δικαίωμα στην ενημέρωση, ώστε να γνωρίζει την ενδεχόμενη υποκλοπή των δεδομένων του[16]. Οι νέοι κανόνες ισχύουν για όλες τις επιχειρήσεις που λειτουργούν στην ΕΕ, έστω και αν -οι εν λόγω επιχειρήσεις- έχουν την έδρα τους εκτός της ΕΕ, αρκεί να αφορούν πολίτες της ΕΕ. Επιπλέον, είναι δυνατόν να

[15] ΕΕ L 191/1, 4.5.2016, σελ. 1-88. Βλ. Ι. Ιγγλεζάκη, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679), εκδ. Interactive Books, (γ΄ εκδ.) 2020· Λ. Κανέλλου, The GDPR Handbook, 2020· Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων. Νέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα, εκδ. Σάκκουλα, 2017· Φ. Παναγοπούλου-Κουτνατζή, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία δεδομένων, εκδ. Σάκκουλα, 2017· Λ. Κοτσαλή/Κ. Μενουδάκο (επιμ.), Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων. Νομική διάσταση και πρακτική εφαρμογή, 2018

[16] Φερενίκη Παναγοπούλου-Κουτνατζή, Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση, Μελέτες, Απόψεις, ΕφημΔΔ-1/2017, σελ. 81

επιβάλλονται διορθωτικά μέτρα, όπως προειδοποιήσεις, εντολές ή πρόστιμα στις επιχειρήσεις που παραβιάζουν τους κανόνες.

Ο ΓΚΠΔ, λόγω του ότι αποτελεί κανονισμό, δεν απαιτεί την έκδοση εφαρμοστικού Νόμου που να ενσωματώνει τις διατάξεις του στην έννομη τάξη κάθε Ευρωπαϊκού Κράτους, δεσμεύοντας άμεσα τα κρατικά του όργανα, τις δημόσιες αρχές και τα δικαστήρια, καθώς και όλα τα πρόσωπα, φυσικά και νομικά, που εμπίπτουν στο πεδίο εφαρμογής του. Παρόλα αυτά, λόγω της διττής του φύσης ως Κανονισμού με στοιχεία Οδηγίας, περιέχει άνω των 70 «ρητρών ευελιξίας» και «ρητρών ανοίγματος» («ρήτρες ρυθμιστικών επιλογών»)[17]. Έτσι, δίδεται η δυνατότητα στα κράτη μέλη με δική τους νομοθεσία να εξειδικεύσουν, να συμπληρώσουν ή να τροποποιήσουν το εσωτερικό τους δίκαιο σύμφωνα με τις ρυθμίσεις του ΓΚΠΔ[18].

3.3.2 Οδηγία 2016/680 (Αστυνομική Οδηγία)

Η οδηγία (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, τέθηκε επίσης σε ισχύ τον Μάιο του 2018. Προστατεύει το θεμελιώδες δικαίωμα των πολιτών για προστασία των δεδομένων προσωπικού χαρακτήρα, όταν αυτά χρησιμοποιούνται από αρχές επιβολής του νόμου. Διασφαλίζει τη δέουσα προστασία των δεδομένων προσωπικού χαρακτήρα των θυμάτων, των μαρτύρων και των υπόπτων εγκλήματος και διευκολύνει τη διασυνοριακή συνεργασία στον αγώνα κατά του εγκλήματος και της τρομοκρατίας.

3.3.3 Οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ)

Η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα

[17] Σπ. Καρύδα, «ΓΚΠΔ και ν. 4624/2019. Μία ιστορική μεταρρύθμιση του εθνικού νομοθετικού πλαισίου για την προστασία του θεμελιώδους δικαιώματος της προστασίας των δεδομένων προσωπικού χαρακτήρα του ατόμου. Νέες προκλήσεις στη σύγχρονη ψηφιακή εποχή. Διάλογος μεταξύ ενωσιακού και εθνικού νομοθέτη», σελ. 5.

[18] Έχει χαρακτηριστεί ως «limping regulation», Βλ. Feiler Lukas, «The EU General Data Protection Regulation (GDPR): A commentary. 5.The relationship with national data protection laws / Working: Globe law and business», 2018.

και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) τροποποιήθηκε από την οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009. Η Οδηγία αυτή εφαρμόζεται στα δημόσια δίκτυα ηλεκτρονικής επικοινωνίας στην Κοινότητα (άρθρο 3 παρ. 1), σ' αυτά εντάσσεται και το διαδίκτυο[19].

3.3.4 Πρόταση Κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες

Η πρόταση για νέο Κανονισμό θα οδηγήσει στην κατάργηση της οδηγίας 2002/58/ΕΚ (Κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) και βρίσκεται επί του παρόντος υπό εξέταση[20]. Ο Κανονισμός ePrivacy αποτελεί ειδικό νόμο (lex specialis) σε σχέση με τον ΓΚΠΔ, συνεπώς θα εξειδικεύσει, θα συμπληρώσει - και πιθανώς σε ορισμένα σημεία θα υπερισχύσει - του ΓΚΠΔ σε ό,τι αφορά δεδομένα ηλεκτρονικών επικοινωνιών που ανταποκρίνονται στον ορισμό των δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο της εντολής του Συμβουλίου, ο Κανονισμός θα καλύπτει το περιεχόμενο ηλεκτρονικών επικοινωνιών που μεταδίδεται μέσω διαθέσιμων στο κοινό υπηρεσιών και δικτύων, καθώς και τα μεταδεδομένα που σχετίζονται με την επικοινωνία, τα οποία θεωρούνται δυνητικά -εξίσου ευαίσθητα- με το περιεχόμενο. Για να εξασφαλιστεί η πλήρης προστασία των δικαιωμάτων ιδιωτικότητας και να προωθηθεί ένα αξιόπιστο και ασφαλές διαδίκτυο των πραγμάτων, οι κανόνες θα καλύπτουν επίσης τα δεδομένα που μεταβιβάζονται μεταξύ μηχανών μέσω δημόσιου δικτύου.

3.3.5 Κανονισμός (ΕΕ) 2018/1725 για την προστασία έναντι της επεξεργασίας δεδομένων από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ και την ελεύθερη κυκλοφορία των δεδομένων αυτών

Ο Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ψηφίστηκε στις 23ης Οκτωβρίου 2018 και έχει ως σκοπό την προστασία των

[19] 2 Βλ. Ιωάννη Δ. Ιγγλεζάκη, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Εκδόσεις Σάκκουλα, Αθήνα, Θεσσαλονίκη, 2003, σελ 205

[20] Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52017PC0010 (τελευταία πρόσβαση 12-2-2021)

φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Με τον κανονισμό αυτό καταργούνται -από την 11 Δεκεμβρίου 2018- ο Κανονισμός 45/2001 και η απόφαση 1247/2002/ΕΚ περί του καθεστώτος και των γενικών όρων άσκησης των καθηκόντων του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ενώ οι παραπομπές στον καταργούμενο κανονισμό και στην καταργούμενη απόφαση θεωρούνται παραπομπές στον νέο Κανονισμό.

Ο νέος Κανονισμός, ακολουθώντας τις αρχές και τους κανόνες του ΓΚΠΔ, θεσπίζει αντίστοιχα μέτρα προστασίας των δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων έναντι των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης. Το πεδίο εφαρμογής των νέων διατάξεων καλύπτει, αφενός την επεξεργασία προσωπικών δεδομένων από τα θεσμικά όργανα, τους οργανισμούς και τις Αρχές της Ένωσης, και αφετέρου τη διαβίβαση των δεδομένων αυτών μεταξύ των θεσμικών αυτών οργάνων, στο βαθμό που αυτό είναι αναγκαίο, λαμβάνοντας υπόψη τους περιορισμούς που ανακύπτουν από Συνθήκες της ΕΕ και τις επιμέρους λειτουργικές ανάγκες και εσωτερικούς κανονισμούς των οργάνων της ΕΕ.

Ορίζεται ρητά το δικαίωμα ενημέρωσης, αλλά και τα λοιπά δικαιώματα των υποκειμένων, τα οποία είναι ίδια με όσα ορίζει ο GDPR και τα περιγράφει αναλυτικά, δίνοντας ιδιαίτερη βαρύτητα στο απόρρητο των ηλεκτρονικών υπηρεσιών. Επίσης, καθορίζεται ο ρόλος των υπευθύνων προστασίας δεδομένων κάθε θεσμικού οργάνου της ΕΕ, καθώς και του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, ο οποίος είναι επιφορτισμένος να διασφαλίζει ότι τα όργανα και οι οργανισμοί της Ένωσης σέβονται τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ιδίως δε το δικαίωμά τους στην προστασία των δεδομένων.

3.3.6 Οδηγία (ΕΕ) 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στην ΕΕ

Η ΕΕ έχει εκδώσει την οδηγία για την ασφάλεια των συστημάτων δικτύου και πληροφοριών[21], η οποία είναι η πρώτη νομική πράξη σε επίπεδο ΕΕ για την ασφάλεια στον κυβερνοχώρο. Σκοπός της οδηγίας είναι, αφενός, η βελτίωση της ασφάλειας στον

[21] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

κυβερνοχώρο σε εθνικό επίπεδο και, αφετέρου, η αύξηση του επιπέδου συνεργασίας εντός της ΕΕ Η οδηγία επιβάλλει επίσης υποχρεώσεις σε φορείς εκμετάλλευσης βασικών υπηρεσιών (συμπεριλαμβανομένων φορέων εκμετάλλευσης στους τομείς της ενέργειας, της υγείας, των τραπεζών, των μεταφορών, των ψηφιακών υποδομών κ.λπ.) και παρόχους ψηφιακών υπηρεσιών για τη διαχείριση των κινδύνων, τη διαφύλαξη της ασφάλειας των οικείων συστημάτων δικτύου και πληροφοριών και την αναφορά συμβάντων που αφορούν την ασφάλεια.

3.3.7 Ειδικές Νομοθετικές πράξεις

Εκτός από τις κύριες νομοθετικές πράξεις για την προστασία των δεδομένων που αναφέρονται παραπάνω, ειδικές διατάξεις για την προστασία των δεδομένων καθορίζονται επίσης σε ειδικές νομοθετικές πράξεις ανά τομέα, όπως ενδεικτικά από το άρθρο 13 σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα της οδηγίας (ΕΕ) 2016/681[22], το κεφάλαιο VI (σχετικά με τις εγγυήσεις προστασίας των δεδομένων) του κανονισμού (ΕΕ) 2016/794[23] και το κεφάλαιο VIII (σχετικά με την προστασία των δεδομένων) του κανονισμού (ΕΕ) 2017/1939 του Συμβουλίου[24].

3.4 Προστασία από το Εθνικό δίκαιο (πέραν του Γενικού Κανονισμού Προσωπικών Δεδομένων)

Πέραν του Πρωτογενούς και Δευτερογενούς Δικαίου της Ευρώπης, που εφαρμόζονται στην Ελλάδα με υπερνομοθετική ισχύ, τα δικαιώματα των υποκειμένων στα προσωπικά δεδομένα, κατοχυρώνονται στην Ελληνική έννομη τάξη και από τα ακόλουθα:

3.4.1 Συνταγματική Προστασία

Η Ελλάδα κύρωσε την ΕΣΔΑ το 1953, ωστόσο το δικτατορικό καθεστώς του 1974 κατήγγειλε τη Σύμβαση, για να κυρωθεί εκ νέου το 1974 κατόπιν ενεργειών της Μεταπολίτευσης. Αργότερα η Ελλάδα, το 1983, υπέγραψε τη Σύμβαση 108 του Συμβουλίου, αλλά την κύρωσε το 1992, αποκτώντας για πρώτη φορά η ελληνική

[22] Το άρθρο ρυθμίζει τα σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.

[23] Το κεφάλαιο αναφέρεται στον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Europol).

[24] Σχετικά με την εφαρμογή ενισχυμένης συνεργασίας για τη σύσταση της Ευρωπαϊκής Εισαγγελίας («ΕΡΡΟ»).

πραγματικότητα δεσμευτικό κείμενο για την προστασία των προσωπικών δεδομένων. Μετέπειτα, ψηφίστηκε ο πρώτος ελληνικός νόμος, ο ν. 2472/1997 για την προστασία των προσωπικών δεδομένων, ως νόμος ενσωμάτωσης της Οδηγίας 95/46/ΕΚ.

Με την αναθεώρηση του ελληνικού Συντάγματος το 2001 προστέθηκε το αρ.9Α Σ που προστατεύει τα προσωπικά δεδομένα και κατοχυρώνει την πληροφοριακή αυτοδιάθεση[25]. Το αρ.9Α Σ προβλέπει ότι "Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως ο νόμος ορίζει"[26]. Στο άρθρο αυτό κατοχυρώνεται το δικαίωμα πληροφορικής αυτοδιάθεσης, καθώς και το δικαίωμα πληροφοριακού αυτοπροσδιορισμού. Επιπλέον, ανατίθεται η προστασία των προσωπικών δεδομένων σε μια ανεξάρτητη αρχή, με τις εγγυήσεις δηλαδή του άρθρου 101^{A} [27]. Η διάταξη αυτή κατοχυρώνει το ατομικό δικαίωμα προστασίας απέναντι στη συλλογή, επεξεργασία και χρήση με συμβατικό ή ηλεκτρονικό τρόπο των προσωπικών δεδομένων[28].

Σχετική είναι και η διάταξη του άρθρου 5Α ως προς το δικαίωμα της πληροφόρησης και του δικαιώματος συμμετοχής στην κοινωνία της πληροφορίας.

3.4.2 Ο Νόμος 2472/97

Η προστασία των προσωπικών δεδομένων είχε ήδη κατοχυρωθεί σε νομοθετικό επίπεδο από το Ν.2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα[29]. Ο Ν.2472/1997, που ενσωμάτωσε την Οδ.95/46/ΕΚ στην ελληνική έννομη τάξη, ρύθμισε το πλαίσιο της επεξεργασίας δεδομένων προσωπικού

---

[25] Βλ. Πρόδρομο Δ. Δαγτόγλου, Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα (Αθήνα: Αντ. Ν. Σάκκουλας, 2012), σελ. 332

[26] Βλ. Πλατής Ειρηνικός, Προσωπικά δεδομένα-Προστασία GDPR, Εκδόσεις Παπαδόπουλος, 2018, σελ. 29

[27] Βλ. Κώστας Χ. Χρυσόγονος, Ατομικά και Κοινωνικά Δικαιώματα, 3η αναθεωρημένη έκδοση, Εκδόσεις Νομική Βιβλιοθήκη, 2006, σελ. 210 και 213

[28] Βλ. Ευ. Βενιζέλος, Το Σύνταγμα του 1975/1986/2001, σχόλιο στο άρθρο 9Α και Ιωάννης Δ. Ιγγλεζάκης, Ευαίσθητα προσωπικά δεδομένα, Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της, ανατύπωση 2004, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη,2004, σελ.56

[29] Βλ. Ν.2472/1997 (ΦΕΚ Α' 50/ 10.04.1997) για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Βλ. επίσης Dr Stavros J. Karageorgiou and Fotini Billiri, "Greece" στο Data Protection Laws of the World, επιμ. Christopher Millard and Mark Ford (London: Sweet & Maxwell, 1998. Για επισκόπηση των εθνικών νομοθεσιών άλλων κρατών σχετικά με την προστασία των προσωπικών δεδομένων, βλ. Dennis Campbell and Joy Fisher, Data Transmission and Privacy (Netherlands: Kluwer Academic Publishers/ Martinus Nijhoff Publishers, 1994), passim.

χαρακτήρα και τα δικαιώματα των υποκειμένων τους, συνέστησε την Ελληνική Αρχή Προστασίας των Προσωπικών Δεδομένων (ΑΠΔΠΧ) και πρόβλεψε διοικητικές και ποινικές κυρώσεις, καθώς και αστική ευθύνη σε περίπτωση παράβασης των διατάξεών του. Εφαρμόζεται σε κάθε επεξεργασία δεδομένων, αυτοματοποιημένη ή μη, φυσικού προσώπου. Η επεξεργασία, γίνεται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ο οποίος είναι εγκατεστημένος στην Ελλάδα ή χρησιμοποιεί μέσα επεξεργασίας ευρισκόμενος στην Ελλάδα. Όπως γίνεται αποδεκτό αντίθετα, δεν εφαρμόζεται όταν πρόκειται για προσωπική χρήση των δεδομένων ή επεξεργασία από Δημόσιες Αρχές σε συγκεκριμένες περιπτώσεις[30].

Ο Ν.2472/1997 συμπληρώθηκε από το Ν.3471/2006 για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες[31]. Ο Ν.3471/2006, που αποτελεί ενσωμάτωση της Οδ.2002/58/ΕΚ, ρύθμισε τους κανόνες επεξεργασίας των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, πρόβλεψε το απόρρητο των ηλεκτρονικών επικοινωνιών, εισήγαγε τα απαιτούμενα μέτρα ασφαλείας, έθεσε κανόνες για την μη ζητηθείσα επικοινωνία και θέσπισε διοικητικές και ποινικές κυρώσεις καθώς και αστική ευθύνη του δημοσίου σε περίπτωση παράβασης των διατάξεών του. Αποτυπώνοντας την τροποποίηση της Οδ.2002/58 από την Οδ.2009/136, ο Ν.4070/2012 τροποποίησε αντιστοίχως το Ν.3471/2006[32].

3.4.3 Ο Νόμος 4624/2019

Ο Νόμος για την προστασία προσωπικών δεδομένων ψηφίστηκε από τη Βουλή των Ελλήνων με τίτλο «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις» και σύμφωνα με το άρθρο 87 του υπό εξέταση νόμου, η ισχύς του άρχισε από την 28η Αυγούστου του 2019.

---

[30] Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα, Εκδόσεις Νομική Βιβλιοθήκη, Θεσσαλονίκη, 2016, σελ. 42.

[31] Βλ. Ν.3471/2006 (ΦΕΚ Α' 133/ 28.06.2006) για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στο τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν.2472/1997.

[32] Βλ. Ν.4070/2012 (ΦΕΚ Α' 82/10.04.2012) με τίτλο: "Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις".

Αξίζει να σημειωθεί ότι η ψήφιση του νέου Νόμου έγινε με τη διαδικασία του κατεπείγοντος και βάση του άρθρου 109 το κανονισμού της Βουλής, καθώς η Ελλάδα κινδύνευε με πρόστιμο από το Δικαστήριο της Ευρωπαϊκής Ένωσης, λόγω της καθυστέρησης στην ενσωμάτωση της Οδηγίας 2016/680[33].

Σκοπός του νόμου είναι: α) η αντικατάσταση του νομοθετικού πλαισίου που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, β) η λήψη μέτρων εφαρμογής του Κανονισμού 2016/679 (ΓΚΠΔ) και γ) η ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

Ο Νόμος δεν έχει αυτοτέλεια σε σχέση με τον Κανονισμό, παρεμβαίνει μόνο σε όσα θέματα του επιτρέπει ο Κανονισμός, επιλύοντας επιμέρους ζητήματα εθνικής σημασίας. Κατά ρητή διατύπωση δε, του άρθρου 84, ο νέος Νόμος καταργεί τον Ν. 2472/1997. Παρόλα αυτά κρίθηκε σκόπιμο να διατηρηθούν σε ισχύ ορισμένες από τις διατάξεις του και αφορούν μεταξύ άλλων σε ορισμούς εννοιών περί της προστασίας δεδομένων προσωπικού χαρακτήρα και διοικητικές κυρώσεις που αφορούν παραβίαση του νόμου για τις ηλεκτρονικές υπηρεσίες (Ν. 3471/2006)[34], όπως αναφέρονται στο ίδιο άρθρο. Επί της ουσίας λοιπόν πρόκειται για μια μερική κατάργηση του «ιδρυτικού» Ν. 2472/1997.

Κατόπιν της πρώτης Γνωμοδότησης της ΑΠΔΠΧ[35] επί των διατάξεων του Νόμου 4624/2019, η Αρχή προέβη σε μία πρώτη θεώρηση της εφαρμογής του ΓΚΠΔ μέσω της λήψης εθνικών νομοθετικών μέτρων και έγιναν ορισμένες παρατηρήσεις όσον αφορά το άρθρο 27 για τα δεδομένα των εργαζομένων, όπως και για την εφαρμογή του Ν. 3471/2006 (ηλεκτρονικές επικοινωνίες). Με την γνωμοδότηση κρίθηκε επίσης ότι, δεν θα τύχουν εφαρμογής από την Αρχή κατά την άσκηση των αρμοδιοτήτων της, οι διατάξεις του Ν. 4624/2019, οι οποίες θα κριθούν ότι έρχονται σε αντίθεση με τον ΓΚΠΔ ή δεν βρίσκουν έρεισμα σε «ρήτρες ανοίγματος – εξειδίκευσης».

[33] Ο οποίος ενσωματώνεται στον Ν. 4624/2019.
[34] Βλ. Νόμος 4624/2019, άρθρο 84
[35] Γνωμοδότηση 1/2020, 24 Ιανουαρίου 2020, ΑΠΔΠΧ

4 ΚΑΝΟΝΕΣ ΑΣΦΑΛΟΥΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Για την καθιέρωση της προστασίας δεδομένων εντός της Ευρωπαϊκής Ένωσης, κρίθηκε αναγκαίο να θεσμοθετηθούν κανόνες, για την εναρμόνιση του επιπέδου προστασίας των προσωπικών δεδομένων των εθνικών νομοθεσιών των κρατών μελών.
Ο Γενικός Κανονισμός για την Προστασία Δεδομένων θεσπίζει, βάσει των αρχών που καθιερώνονται στο άρθρο 5 του Κανονισμού, ένα επίπεδο αναλυτικών κανόνων, οι οποίοι είναι άμεσα εφαρμοστέοι στις εθνικές έννομες τάξεις.

4.1 Υποχρέωση διασφάλισης ασφαλούς επεξεργασίας

Οι κανόνες για την ασφάλεια της επεξεργασίας, όπως αυτοί προσδιορίζονται ρητά στο άρθρο 32 ΓΔΚΠ ορίζουν τις υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία για ασφαλή επεξεργασία και αποφυγή της μη εξουσιοδοτημένης επέμβασης, ενώ η γενικότερη ευθύνη του για τον προσδιορισμό των κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει τη νομιμότητα μιας επεξεργασίας πηγάζει και από το άρθρο 24 ΓΚΠΔ.

Το αναγκαίο επίπεδο ασφάλειας των δεδομένων σύμφωνα με την διάταξη του άρθρου 32 ΓΔΚΠ καθορίζεται από (1) τις τελευταίες εξελίξεις, υπό την έννοια ότι πρέπει να αξιολογούνται τα χαρακτηριστικά ασφάλειας τα οποία είναι διαθέσιμα στην ενίοτε αγορά για κάθε συγκεκριμένο τύπο επεξεργασίας, (2) το κόστος εφαρμογής, καθώς δεν μπορεί να θεωρείται επιβεβλημένη μια διαδικασία που απαιτεί μεγάλο κόστος ενσωμάτωσης και συντήρησης, (3) τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας της κάθε περίπτωσης και (4) τους κινδύνους που ενέχει η κάθε επεξεργασία για θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των προσωπικών δεδομένων.

Βάσει τόσο του Γενικού Κανονισμού για την Προστασία Δεδομένων, όσο και του δικαίου του Συμβουλίου της Ευρώπης[36], οι υπεύθυνοι επεξεργασίας έχουν γενική υποχρέωση διαφάνειας και λογοδοσίας,[37] όταν επεξεργάζονται δεδομένα προσωπικού

[36] Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 1

[37] Ι. Ιγγλεζάκης, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Ο Γενικός Κανονισμός προστασίας Προσωπικών Δεδομένων, (γ΄εκδ.) 2020, σελ. 187 επ· Λ. Μήτρου, Ο γενικός Κανονισμός προστασίας προσωπικών Δεδομένων, σελ. 91 επ.

χαρακτήρα και ιδιαιτέρως, όταν εμφανίζονται παραβιάσεις δεδομένων. Σε περιπτώσεις που πραγματοποιήθηκαν παραβιάσεις προσωπικών δεδομένων, οι υπεύθυνοι επεξεργασίας οφείλουν να ενημερώνουν τις εποπτικές αρχές σε ρητά προβλεπόμενους χρόνους, εκτός εάν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για δικαιώματα και ελευθερίες φυσικών προσώπων. Τα υποκείμενα των δεδομένων θα πρέπει σε περίπτωση παραβίασης να ενημερώνονται σχετικά, όταν αυτή ενδέχεται να θέσει σε μεγάλο κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Ο ΓΚΠΔ ορίζει επίσης ότι τα φυσικά πρόσωπα θα πρέπει να έχουν τον έλεγχο των δικών τους δεδομένων προσωπικού χαρακτήρα και ότι θα πρέπει να ενισχυθούν η ασφάλεια δικαίου και η πρακτική ασφάλεια για τα φυσικά πρόσωπα, τους οικονομικούς παράγοντες και τις δημόσιες αρχές[38]. Η επεξεργασία όμως δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία και ανάλογη για τους σκοπούς της διασφάλισης της ασφάλειας δικτύων και πληροφοριών, αποτελεί έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων και επιτρέπεται[39].

Όσον αφορά την κατάρτιση προφίλ, ο ΓΚΠΔ ορίζει ότι, το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να μην υπόκειται σε απόφαση, η οποία μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, κυρίως δηλαδή την «κατάρτιση προφίλ» που αποτελείται από οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα[40]. Η λήψη της απόφασης αυτής «που βασίζεται σε αυτήν την επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, θα πρέπει να επιτρέπεται μόνο όταν προβλέπεται ρητά από το δίκαιο της Ένωσης ή κράτους μέλους για σύννομο σκοπό», όπως κάποιοι από αυτούς αναφέρονται στον ΓΚΠΔ ενδεικτικά[41]. Η επεξεργασία αυτή όμως πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, οι οποίες είναι υποχρεωτικό να περιλαμβάνουν ειδική ενημέρωση του υποκειμένου των δεδομένων και το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, το δικαίωμα διατύπωσης της άποψης του, το δικαίωμα να λάβει αιτιολόγηση της

[38] Βλ. Αιτιολογική σκέψη 7 ΓΚΠΔ
[39] Βλ. Αιτιολογική σκέψη 49 ΓΚΠΔ
[40] Βλ. Αιτιολογική σκέψη 71 ΓΚΠΔ
[41] Μεταξύ άλλων η αιτιολογική σκέψη 71, αναφέρεται για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής σύμφωνα με τους κανονισμούς, τα πρότυπα και τις συστάσεις των θεσμικών οργάνων της Ένωσης ή των εθνικών οργάνων εποπτείας και προκειμένου να διασφαλιστεί η ασφάλεια και η αξιοπιστία της υπηρεσίας που παρέχει ο υπεύθυνος επεξεργασίας, ή όταν είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ υποκειμένου των δεδομένων και υπευθύνου επεξεργασίας ή όταν το υποκείμενο των δεδομένων παρέσχε τη ρητή συγκατάθεσή του

απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης και το δικαίωμα αμφισβήτησης της απόφασης και μόνο σε περιπτώσεις ενηλίκων.

Η αιτιολογική σκέψη 78 ορίζει ότι «η προστασία των δικαιωμάτων και των 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»[42]. Στα πλαίσια τους ασφαλούς σχεδιασμού ο Κανονισμός ενθαρρύνει να λαμβάνονται υπόψη οι τελευταίες εξελίξεις και να διασφαλίζεται ότι οι υπεύθυνοι και οι εκτελούντες την επεξεργασία, θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την ασφαλή επεξεργασία και την προστασία των δεδομένων.

Στην αιτιολογική σκέψη 81 όσον αφορά την επεξεργασία από τον εκτελούντα την επεξεργασία, ορίζεται ότι ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί μόνο εκτελούντες επεξεργασία οι οποίοι παρέχουν επαρκείς διαβεβαιώσεις, ιδίως από πλευράς εμπειρογνωμοσύνης, αξιοπιστίας και πόρων, για την εφαρμογή τεχνικών και οργανωτικών μέτρων που θα ανταποκρίνονται στις απαιτήσεις του παρόντος κανονισμού, συμπεριλαμβανομένων εκείνων που αφορούν την ασφάλεια της επεξεργασίας. Ο καθένας τους ορίζεται επίσης ότι προκειμένου να διατηρηθεί η ασφάλεια και να αποφευχθεί η επεξεργασία κατά παράβαση του κανονισμού, θα πρέπει «να αξιολογεί τους κινδύνους που ενέχει η επεξεργασία και να εφαρμόζει μέτρα για τον μετριασμό των εν λόγω κινδύνων, όπως για παράδειγμα μέσω κρυπτογράφησης. Τα εν λόγω μέτρα θα πρέπει να διασφαλίζουν κατάλληλο επίπεδο ασφάλειας, πράγμα που περιλαμβάνει και την εμπιστευτικότητα, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις και το κόστος της εφαρμογής σε σχέση με τους κινδύνους και τη φύση των δεδομένων προσωπικού χαρακτήρα που πρέπει να προστατευθούν»[43]. Μνεία γίνεται επίσης και στην εκτίμηση κινδύνου στην οποία πρέπει να δίνεται προσοχή στους ενδεχόμενους κινδύνους που μπορεί να προκύψουν και θα μπορούσαν να οδηγήσουν σε σωματική, υλική ή μη υλική βλάβη.

[42] Επίσης ορίζεται ότι «Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα το 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 ασφάλειας»

[43] Βλ. Αιτιολογική σκέψη 83 ΓΚΠΔ

4.2 Τρόποι διασφάλισης ασφάλειας δεδομένων

Το άρθρο 32 παράγραφος 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων αναφέρει 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 διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων[44].

Τα μέτρα αυτά περιλαμβάνουν, μεταξύ άλλων, τα εξής: (1) Ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα[45]· (2) Διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας[46]· (3) Αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση απώλειας δεδομένων[47]· (4) Διαδικασία για τη δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των μέτρων για τη διασφάλιση της επεξεργασίας[48]· (5) Χρήση εγκεκριμένου κώδικα δεοντολογίας[49]· (6) Διαδικασίες χειρισμού περιστατικών παραβίασης[50].

Παρόμοια διάταξη προβλέπεται και από την Εκσυγχρονισμένη Σύμβαση 108, όπου αναφέρεται ότι κάθε συμβαλλόμενος μεριμνά, ώστε ο υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκτελών την επεξεργασία να λαμβάνει κατάλληλα μέτρα ασφάλειας κατά κινδύνων όπως η τυχαία ή μη εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και η καταστροφή, η απώλεια, η χρήση, η τροποποίηση ή η κοινολόγηση των δεδομένων αυτών[51].

[44] Ό.π., άρθρο 32 παράγραφος 1
[45] Ό.π., άρθρο 32 παράγραφος 1 στοιχείο α΄
[46] Ό.π., άρθρο 32 παράγραφος 1 στοιχείο β.
[47] Ό.π., άρθρο 32 παράγραφος 1 στοιχείο γ.
[48] Ό.π., άρθρο 32 παράγραφος 1 στοιχείο δ.
[49] Ό.π., άρθρο 32 παράγραφος 3 σε συνδυασμό με άρθρο 40 και άρθρο 42 ΓΚΠΔ
[50] Ό.π., άρθρο 32 παράγραφος 4
[51] Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 1.

Βάσει και των ρυθμίσεων και των δύο αυτών άρθρων ορίζεται ότι, σε περίπτωση παραβίασης δεδομένων η οποία ενδέχεται να έχει αντίκτυπο στα δικαιώματα και στις ελευθερίες φυσικών προσώπων, ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει την εποπτική αρχή για την παραβίαση[52].

Για την εξασφάλιση της ασφάλειας των δεδομένων δεν αρκεί όμως μόνο η ύπαρξη των ανωτέρω αναφερόμενων ενδεικτικά τεχνικών μέτρων και η χρήση κατάλληλου εξοπλισμού, υλισμικού και λογισμικού. Απαιτείται να υπάρχουν σε κάθε οργανισμό και κατάλληλοι εσωτερικοί κανόνες οργάνωσης. Οι κανόνες αυτοί ιδανικά θα πρέπει να ρυθμίζουν μια σειρά από θέματα, όπως την τακτική παροχή πληροφοριών στους υπαλλήλους για τους εφαρμοζόμενους κανόνες, την σαφή κατανομή αρμοδιοτήτων, σαφή περιγραφή καθηκόντων και διασφάλιση εξουσιοδότησης προς τους υπαλλήλους, την χρήση δεδομένων προσωπικού χαρακτήρα μόνο σύμφωνα με τις εντολές του αρμόδιου προσώπου, την προστασία της πρόσβασης σε χώρους, όπου υπάρχει ευαίσθητο τεχνολογικό υλικό, την χρήση αυτοματοποιημένων πρωτοκόλλων σχετικά με την ηλεκτρονική πρόσβαση και την προσεκτική τεκμηρίωση άλλων μορφών κοινοποίηση,ς όταν αυτές δεν γίνονται αυτοματοποιημένα.

4.2.1 Διεθνή Πρότυπα και Οργανισμός ENISA

Το πλαίσιο προστασίας της ασφάλειας πληροφοριών καθορίζεται από ένα σύνολο θεσμικών ρυθμίσεων, όπως κανονιστικές και νομικές. Κανονιστική ρύθμιση αποτελεί η καθιέρωση προτύπων (standards) όπως και οι κώδικες δεοντολογίας οι οποίοι συμπληρώνουν την υπάρχουσα νομοθεσία. Πρότυπο για παράδειγμα αποτελεί ένα τεχνικό πρότυπο (technical standard), το οποίο είναι ένα σύνολο αποδεκτών κριτηρίων, μεθόδων και διεργασιών ή πρακτικών.

Τα πρότυπα μπορεί να προκύπτουν από σύνολο εταιρειών ή οργανισμών προτυποποίησης κατόπιν έρευνας και ευρύτερης συμφωνίας, δηλαδή de jure πρότυπα. Υπάρχουν όμως και γενικά πρότυπα τα οποία γίνονται ευρέως αποδεκτά, χωρίς να είναι μέρος ενός τυπικού κανονιστικού πλαισίου.

Για αυτά τα πρότυπα δεν έχει κανείς τη νομική ή κανονιστική υποχρέωση να τα ακολουθήσει, γνωστά ως de facto πρότυπα και αποτελούν τα ισχυρότερα πρότυπα στην πράξη, καθώς επικράτησαν μετά από ανταγωνισμό.

[52] Βλ. παρακάτω ενότητα 5.4 Υποχρεώσεις γνωστοποίησης παραβίασης δεδομένων

Η διεργασία ανάπτυξης και υλοποίησης τεχνικών προτύπων ονομάζεται Προτυποποίηση. Η συμμόρφωση ενός οργανισμού με κάποιο πρότυπο εξασφαλίζει την ύπαρξη συγκεκριμένων επιθυμητών χαρακτηριστικών σε προϊόντα ή υπηρεσίες. Επίσης, με αυτό το τρόπο διασφαλίζεται η συμβατότητα και η διαλειτουργικότητα μεταξύ διαφορετικών πληροφοριακών συστημάτων. Για να εξασφαλιστεί η συμμόρφωση ενός οργανισμού με συγκεκριμένες προδιαγραφές θα πρέπει αυτός να αξιολογείται με σκοπό την απόκτηση του αντίστοιχου πιστοποιητικού συμμόρφωσης (πιστοποίηση). Η πιστοποίηση ορίζει τις διαδικασίες αξιολόγησης και ελέγχου ενός οργανισμού. Από τα πλέον διαδεδομένα πρότυπα ασφάλειας πληροφοριών είναι η σειρά προτύπων ISO/IEC 27000, τα ISO/IEC 29151, Control Objectives for Information Technology (CobIT) καθώς και τα Common Criteria. Επίσης, υπάρχουν τα εθνικά πρότυπα (π.χ. NIST/SP 800-53) και λίστες εποπτικών αρχών ή άλλων οργανισμών (π.χ. ENISA) που μπορεί να χρησιμοποιήσει ένας οργανισμός. Στον τομέα των διευρωπαϊκών δικτύων στις τηλεπικοινωνίες (Trans-European Telecommunications Networks) υπάρχει το European Privacy Seal (σφραγίδα σεβασμού των προσωπικών δεδομένων, EuroPriSe)[53], το οποίο διερευνά τις δυνατότητες πιστοποίησης προϊόντων, ιδίως λογισμικού, για τη διευκόλυνση της συμμόρφωσης με το ευρωπαϊκό δίκαιο για την προστασία δεδομένων.

4.2.1.1 Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) συστάθηκε για τη βελτίωση της ικανότητας της ΕΕ, των κρατών μελών της ΕΕ και της επιχειρηματικής κοινότητας να προλαμβάνουν, να αντιμετωπίζουν και να αποκρίνονται σε προβλήματα ασφάλειας δικτύων και πληροφοριών[54]. Ο ENISA δημοσιεύει τακτικά αναλύσεις για τις τρέχουσες απειλές ασφάλειας, καθώς και συμβουλές για τους τρόπους αντιμετώπισής τους[55]. Τον Σεπτέμβριο του 2017 η Ευρωπαϊκή Επιτροπή πρότεινε σχέδιο κανονισμού με σκοπό τη μεταρρύθμιση της εντολής του ENISA, προκειμένου να ληφθούν υπόψη οι νέες αρμοδιότητες και τα νέα καθήκοντα του

[53] Βλ. https://www.euprivacyseal.com/ (τελευταία πρόσβαση 12-2-2021)

[54] Κανονισμός (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013, σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004 (ΕΕ L 165 της 18.6.2013, σ. 41).

[55] Για παράδειγμα, ENISA (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations· ENISA (2016), Security of Mobile Payments and Digital Wallets.

Οργανισμού βάσει της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Σκοπός του προτεινόμενου κανονισμού είναι η διεύρυνση των καθηκόντων του ENISA και η ενίσχυση του ρόλου του ως «σημείου αναφοράς στο οικοσύστημα της ΕΕ για την ασφάλεια στον κυβερνοχώρο»[56]. Ο προτεινόμενος Κανονισμός δεν θα πρέπει να θίγει τις αρχές του ΓΚΠΔ, και αποσαφηνίζοντας τα αναγκαία στοιχεία που συνθέτουν τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, και επιπλέον θα πρέπει να ενισχύει την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Παράλληλα, τον Σεπτέμβριο του 2017 η Ευρωπαϊκή Επιτροπή πρότεινε σχέδιο εκτελεστικού κανονισμού για τον προσδιορισμό των στοιχείων που λαμβάνουν υπόψη οι πάροχοι ψηφιακών υπηρεσιών, ώστε να διαφυλάσσουν την ασφάλεια των οικείων συστημάτων δικτύου και πληροφοριών, όπως προβλέπεται στο άρθρο 16 παράγραφος 8 της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Κατά τον χρόνο σύνταξης της παρούσας μελέτης, οι συζητήσεις σχετικά με τις δύο αυτές προτάσεις βρίσκονταν σε εξέλιξη.

4.3 Εμπιστευτικότητα

Ο ΓΚΠΔ αναφέρεται στην εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα καταρχήν στο πλαίσιο γενικής αρχής[57]. Σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο στ', τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να 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 («ακεραιότητα και εμπιστευτικότητα»).
Στο άρθρο 32 του ΓΚΠΔ, επίσης ορίζεται ότι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία οφείλουν να εφαρμόζουν τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται υψηλό επίπεδο ασφάλειας. Τα μέτρα αυτά περιλαμβάνουν, μεταξύ άλλων, την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα, τη δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και

[56] Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο» και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»), COM(2017) 477 της 13ης Σεπτεμβρίου 2017, σ. 6.
[57] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο στ'.

της αξιοπιστίας της επεξεργασίας σε συνεχή βάση, την αξιολόγηση και τη δοκιμή της αποτελεσματικότητας των μέτρων και τη δυνατότητα αποκατάστασης της επεξεργασίας σε περίπτωση φυσικού ή τεχνικού συμβάντος. Επιπλέον, η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης μπορεί να χρησιμοποιηθεί ως στοιχείο, για να αποδειχθεί η συμμόρφωση προς την αρχή της ακεραιότητας και της εμπιστευτικότητας. Επίσης, σύμφωνα με το άρθρο 28 του ΓΚΠΔ, η σύμβαση που συνδέει τον υπεύθυνο επεξεργασίας με τον εκτελούντα την επεξεργασία πρέπει να προβλέπει ότι ο εκτελών την επεξεργασία θα διασφαλίσει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα εκ του νόμου υποχρέωση τήρησης εμπιστευτικότητας.

Τα παραπάνω άρθρα παρότι αφορούν την εμπιστευτικότητα, αναφέρονται σε δύο διαφορετικές έννοιες[58]. Το άρθρο 5 παράγραφος 1 στοιχείο στ' αναφέρεται στην ανάγκη προστασίας των προσωπικών δεδομένων, όπως αυτά ορίζονται στο άρθρο 4 παράγραφος 1, δηλαδή ως πληροφορίες που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ενώ τα άρθρα 32 και 28, αναφέρονται στην υποχρέωση τήρησης εμπιστευτικότητας. Εμπιστευτικές πληροφορίες αποτελούν οι ορισμένες πληροφορίες που σχετίζονται στενά με την δραστηριότητα μίας επιχείρησης. Οι εμπιστευτικές αυτές πληροφορίες μπορεί να χρίζουν προστασίας ως αντικείμενα συγκεκριμένων δικαιωμάτων, όπως πνευματικής ιδιοκτησίας ή να αποτελούν εμπορικά και βιομηχανικά απόρρητα και σε κάθε περίπτωση βρίσκονται στην σφαίρα του απόλυτου ελέγχου του κατόχου των πληροφοριών. Τα προσωπικά δεδομένα αντίθετα, ανήκουν αποκλειστικά στα υποκείμενα των δεδομένων αυτών και ως έννοια δεν μπορούν να θεωρηθούν σε καμία περίπτωση ιδιοκτησία ή περιουσία ενός υπεύθυνου επεξεργασίας ακόμη και όταν περιέχονται σε συστήματα ή μέσα των οποίων αποκλειστικός ιδιοκτήτης είναι ο υπεύθυνος επεξεργασίας.

Ο ΓΚΠΔ εισάγει κανόνες ασφάλειας επεξεργασίας και όχι εμπιστευτικότητας πληροφοριών για τις οποίες προβλέπεται συνήθως κάποια σύμβαση εμπιστευτικότητας μεταξύ των μερών που διαβιβάζουν πληροφορίες. Γι αυτό το λόγο οι κανόνες και οι υποχρεώσεις που εισάγει ο ΓΚΠΔ αλλά και η συνολική νομοθεσία των προσωπικών

[58] Η. Τσαούσης, Τέσσερα αμφιλεγόμενα ζητήματα κατά την εφαρμογή του GDPR, ΕΠΙΧΕΙΡΗΣΗ, Τεύχος 174/2020, Οκτώβριος 2020, κεφ. ΙΙΙ. Εμπιστευτικότητα, σελ. 836επ.

δεδομένων εφαρμόζονται αυτοδικαίως σε κάθε αποδέκτη των δεδομένων, ανεξαρτήτως της ύπαρξης οποιασδήποτε διμερούς συμβατικής σχέσης, καθώς αποσκοπεί στην προστασία όλων των υποκειμένων των δεδομένων. Αντίθετα, στην προστασία των εμπιστευτικών πληροφοριών, ο κάτοχος αυτών είναι σε θέση να δεσμεύσει συμβατικά τον αποδέκτη των πληροφοριών ως προς την τήρηση συγκεκριμένων υποχρεώσεων εμπιστευτικότητας, συνάπτοντας με τον αποδέκτη σχετική σύμβαση εμπιστευτικότητας.

Στις διατάξεις των άρθρων 32 και 28 καθίσταται σαφές ότι το απόρρητο αναφέρεται σε συστήματα και υπηρεσίες επεξεργασίας και όχι στα δεδομένα αυτά καθαυτά και η ίδια λογική διέπει και τις άλλες διατάξεις, αφού πουθενά δεν γίνεται ευθέως λόγος για «εμπιστευτικά» προσωπικά δεδομένα, αλλά αντίθετα γίνεται σαφές ότι ο σκοπός των σχετικών ρυθμίσεων είναι η ασφάλεια της επεξεργασίας και η αποτροπή της απώλειας των δεδομένων ή την αθέμιτης πρόσβασης τρίτων στα συστήματα επεξεργασίας δεδομένων. Ο ΓΚΠΔ αναφέρεται σαφώς στην ασφάλεια των συστημάτων και υπηρεσιών επεξεργασίας και όχι στα ίδια τα προσωπικά δεδομένα και πώς άλλωστε θα μπορούσε να επιβάλει την τήρηση των προσωπικών δεδομένων ως εμπιστευτικών από την στιγμή που από την φύση τους πολλά από αυτά είναι ευρέως γνωστά αλλά ούτε και εισάγεται με τον Κανονισμό κάποιο κριτήριο διαχωρισμού μεταξύ εμπιστευτικών και μη εμπιστευτικών δεδομένων. Επιπλέον, η διαβίβαση των προσωπικών δεδομένων είναι μορφή επεξεργασίας και δεν είναι δυνατόν να αποκλειστεί συμβατικά εφόσον τηρούνται οι προϋποθέσεις που θέτει ο Κανονισμός για την επεξεργασία τους, όπως την αρχή του περιορισμού του σκοπού, δηλαδή εφόσον η διαβίβαση των δεδομένων γίνεται εντός του πλαισίου των σκοπών για τους οποίους τα δεδομένα αυτά συλλέχθηκαν αλλά και των άλλων απαιτούμενων κατά περίπτωση αρχών, όπως της ελαχιστοποίησης, διαφάνειας κλπ.

Η υποχρέωση εμπιστευτικότητας δεν εκτείνεται σε καταστάσεις στις οποίες τα δεδομένα περιέρχονται σε γνώση κάποιου που ενεργεί ως ιδιώτης και όχι ως εντολοδόχος του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Στην περίπτωση αυτή, τα άρθρα 32 και 28 του ΓΚΠΔ δεν εφαρμόζονται, καθώς η χρήση δεδομένων προσωπικού χαρακτήρα από ιδιώτες εξαιρείται πλήρως από το πεδίο εφαρμογής του κανονισμού[59]. Η εξαίρεση λόγω οικιακής δραστηριότητας αφορά τη χρήση δεδομένων προσωπικού χαρακτήρα «από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής

[59] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 2 στοιχείο γ'.

δραστηριότητας». Ωστόσο, μετά την απόφαση του ΔΕΕ στην υπόθεση *Bodil Lindqvist*[60], η εξαίρεση αυτή πρέπει να ερμηνεύεται συσταλτικά, ιδίως όσον αφορά την κοινοποίηση δεδομένων, καθώς δεν επεκτείνεται, όταν υπάρχει δημοσιοποίηση σε απεριόριστο αριθμό αποδεκτών στο διαδίκτυο ή όταν υπάρχει διαφορετικός σκοπός χρήσης που εμπίπτει σε επαγγελματική δραστηριότητα.

Μια άλλη πτυχή της εμπιστευτικότητας είναι η «εμπιστευτικότητα των επικοινωνιών», η οποία ρυθμίζεται από lex specialis. Οι ειδικοί κανόνες για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών βάσει της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες επιβάλλουν στα κράτη μέλη να απαγορεύουν την ακρόαση, την υποκλοπή, την αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών μεταδεδομένων από πρόσωπα πλην των χρηστών ή χωρίς τη συγκατάθεση των χρηστών[61]. Το εθνικό δίκαιο μπορεί να επιτρέπει εξαιρέσεις από την αρχή αυτή μόνο για λόγους εθνικής ασφάλειας, άμυνας, πρόληψης ή ανίχνευσης εγκλημάτων, και μόνο εάν τα μέτρα αυτά είναι αναγκαία και ανάλογα προς τους επιδιωκόμενους σκοπούς[62]. Οι ίδιοι κανόνες θα ισχύουν στο πλαίσιο του μελλοντικού κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

4.4 Ακεραιότητα

Ακεραιότητα αποτελεί η διασφάλιση της πληρότητας και της ορθότητας των δεδομένων, ώστε να παραμένουν ακριβή, ακέραια και ενημερωμένα και να προστατεύονται από μη εξουσιοδοτημένη μεταβολή τους. Η υποχρέωση προστασίας της, πηγάζει από το άρθρο 5 παράγραφος 1 στοιχείο στ΄ και άρθρο 32 ΓΚΠΔ, όπως και από το άρθρο 7 της Εκσυγχρονισμένης Σύμβασης 108.

Αυτή η έννοια της ακεραιότητας, όπως εκφράζεται στα παραπάνω νομοθετικά κείμενα που αφορούν την ιδιωτικότητα, έχει να κάνει καθαρά με θέματα διαφύλαξης δεδομένων των υποκειμένων και είναι τελείως διαφορετική όπως νοείται στο Σύνταγμα στο άρθρο 5, όπου εκφράζεται ως έννοια του πυρήνα της προσωπικότητας του ατόμου, ως προστατευόμενου αγαθού, με τη φυσική και την ηθική της διάσταση και ως επακόλουθο αυτής η εξωτερίκευσή της στην κοινωνικο-οικονομική σφαίρα με τη μορφή αγαθών. Το

[60] ΔΕΕ, C-101/01, Ποινική δίκη κατά Bodil Lindqvist, 6 Νοεμβρίου 2003.
[61] Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, άρθρο 5 παράγραφος 1.
[62] Ό.π., άρθρο 15 παράγραφος 1.

δικαίωμα αυτό στην προσωπικότητα, όταν προσβληθεί είναι δυνατόν να γεννήσει οικονομικές αξιώσεις, αντίθετα με την οριζόμενη έννοια στον τομέα της ιδιωτικότητας, όπου σημασία έχει η έννοια της ταυτότητας του προσώπου και όλων εκείνων των χαρακτηριστικών που καθιστούν κάθε άτομο ποιοτικά διαφορετικό. Συνεπώς σε περιπτώσεις προσβολής του δικαιώματος στην ιδιωτικότητα, αυτό που ουσιαστικά προσβάλλεται είναι η δυνατότητα του προσώπου να διαμορφώνει την ταυτότητα και την ηθική του υπόσταση, με όρους ελευθερίας και αυτονομίας.

Με την έννοια αυτή στην ασφάλεια πληροφοριών, ακεραιότητα αποτελεί, η διασφάλιση ότι η κάθε πληροφορία είναι πλήρης, ακριβής και έγκυρη (βλ. κεφ. 5.1). Για την πληρότητα των δεδομένων έχει σημασία να είναι ορθά τα δεδομένα που συλλέγονται από το ίδιο το υποκείμενο και από τρίτες πηγές. Αυτές θα πρέπει να διασφαλίζεται ότι παρέχουν έγκυρες και επικαιροποιημένες πληροφορίες. Η ακρίβεια στα δεδομένα εξασφαλίζεται μέσω της καθιέρωσης εντός των οργανισμών, διαδικασιών ενημέρωσης των δεδομένων που διατηρούνται, είτε μέσω της χρήσης αυτοματοποιημένων συστημάτων που μπορούν να ενημερώνουν εγκαίρως τον υπεύθυνο επεξεργασίας για την εκάστοτε ανάγκη επικαιροποίησης, είτε μέσω της ύπαρξης μιας διαδικασίας ενημέρωσης των υποκειμένων και διαγραφής των στοιχείων που δεν μπορεί να αποδειχθεί ότι έχει ληφθεί μέριμνα ως προς την ακρίβειά τους.

Για να θεωρούνται έγκυρα τα δεδομένα απαιτείται αυτά να μην έχουν αλλοιωθεί είτε κατά την διατήρηση είτε κατά της διαβίβαση. Αλλοίωση μπορεί να προκληθεί από την απώλεια της ακεραιότητας της πληροφορίας που προκύπτει από τη μη εξουσιοδοτημένη εισαγωγή, τροποποίηση ή διαγραφή τμήματος ή του συνόλου της πληροφορίας που τηρείται σε έναν οργανισμό. Αυτή μπορεί να συμβεί εκουσίως, όταν υπάρχει επίθεση από τρίτο με σκοπό την υποκλοπή ή αλλοίωση των δεδομένων ή ακουσίως λόγω ελλιπούς λήψεως μέτρων ασφαλείας ή διαδικασιών. Επαρκή κάλυψη κατά εκουσίων αλλοιώσεων μπορεί να θεωρηθεί η λήψη μέτρων ασφαλείας, όπως τεχνολογιών αποτροπής επιθέσεων ή ασφαλών διαβιβάσεων και επαλήθευσης ακεραιότητες δεδομένων. Οι ακούσιες αλλοιώσεις μπορούν να αντιμετωπιστούν με την λήψη οργανωτικών μέτρων και διαδικασιών φυσικής προστασίας, όπως τακτική λήψη αντιγράφων σε υπηρεσίες cloud με χρήση κρυπτογραφίας ή ψευδωνυμοποίησης [63]. Ένας

[63] Οι βέλτιστοι τρόποι αποφυγής αλλοίωσης δεδομένων σύμφωνα με Ι. Μαυρίδη είναι: 1. η αξιοποίηση μηχανισμών συναρτήσεων κατακερματισμού, 2. η χρήση ψηφιακών υπογραφών, 3. η χρήση ισχυρών

από τους βασικούς σκοπούς της χρήσης της κρυπτογραφίας είναι άλλωστε η προστασία της εμπιστευτικότητας και της ακεραιότητας, ώστε τα δεδομένα να μπορούν να τροποποιηθούν – αλλοιωθούν μόνο από εξουσιοδοτημένα μέλη του κάθε οργανισμού και η ύπαρξη τρόπου ανίχνευσης της αλλοίωσης (βλ. κεφ. 6.2).

Το επίπεδο προστασίας της ακεραιότητας των δεδομένων, επίσης πρέπει να ανταποκρίνεται στην σημαντικότητα των προστατευόμενων δεδομένων αλλά και του κινδύνου που θα επιφύλασσε τυχόν απώλειά της. Στα προσωπικά δεδομένα ειδικών κατηγοριών, απαιτείται η λήψη επιπλέον μέτρων της εμπιστευτικότητας και της ακεραιότητας[64].

4.5 Υποχρεώσεις γνωστοποίησης παραβίασης δεδομένων

Παραβίαση δεδομένων προσωπικού χαρακτήρα θεωρείται όταν υπάρχει τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση δεδομένων προσωπικού χαρακτήρα ή πρόσβαση σε αυτά κατά την επεξεργασία[65]. Παρότι οι νέες τεχνολογίες, παρέχουν πλέον περισσότερες δυνατότητες για την εγγύηση της ασφάλειας της επεξεργασίας, οι παραβιάσεις των δεδομένων παραμένουν συχνές. Τα αίτια των παραβιάσεων μπορούν να ποικίλλουν και μπορεί να περιλαμβάνουν λάθη του ανθρώπινου παράγοντα, από αμέλεια ή δόλο ή εξωτερικές ηλεκτρονικές ή φυσικές απειλές.

Η απώλεια της εμπιστευτικότητας των δεδομένων που ενδεχομένως πραγματοποιηθεί, μπορεί να αφορά την ιδιωτική ζωή ή την προστασία δεδομένων φυσικών προσώπων και να οδηγήσουν σε πληθώρα ζημιών όπως υλική ή οικονομική, απάτη, υποκλοπή στοιχείων, παραβίαση επαγγελματικού απορρήτου όπως και ζημία στη φήμη του υποκειμένου των δεδομένων. Η Ομάδα εργασίας του άρθρου 29 (ήδη Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων) σε κατευθυντήριες γραμμές σχετικά με

μηχανισμών αυθεντικοποίησης και 4. η χρήση πρωτοκόλλων που παρέχουν προστασία της ακεραιότητας του κάθε μεταδιδόμενου μηνύματος. Ι. Μαυρίδης, Ασφάλεια Πληροφοριών στο Διαδίκτυο, 2005, κεφ. 5, σελ. 94

[64] Πρακτικές που προτείνονται από τον Ι. Μαυρίδη στην προστασία των προσωπικών δεδομένων ειδικών κατηγοριών είναι, 1. Αποθήκευση μόνο των ευαίσθητων δεδομένων που είναι απαραίτητα για την εκάστοτε λειτουργία της εφαρμογής, 2. Αποφυγή αποθήκευσης ευαίσθητων δεδομένων μέσα στον κώδικα της εφαρμογής, 3. Κρυπτογραφημένη αποθήκευση των ρυθμίσεων σύνδεσης σε συστήματα διαχείρισης βάσεων δεδομένων, συνθηματικών, κλειδιών κρυπτογράφησης κλπ, 4. Εκτεταμένη χρήση κρυπτογραφικών τεχνικών. κεφ. 5.4.5, ο.π. σελ. 97

[65] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 12· βλ. επίσης Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP250rev.01, 3 Οκτωβρίου 2017, σ. 8

τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα έχει κρίνει ότι υπάρχουν τριών ειδών επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα: η κοινοποίηση, η απώλεια και η μεταβολή[66]. Ανεξάρτητα από την ανάγκη λήψης μέτρων για αποκατάσταση του επιπέδου ασφάλειας των δεδομένων που έχουν παραβιαστεί, υπάρχει παράλληλα η υποχρέωση καταγραφής στην συμμόρφωση κάθε οργανισμού του περιστατικού ασφαλείας, ανεξαρτήτως των επιπτώσεων που μπορεί να είχε άμεσα, έτσι ώστε να μπορεί να χρησιμοποιηθεί αργότερα ως μέσο απόδειξης της ορθής αντιμετώπισης του περιστατικού από τον υπεύθυνο επεξεργασίας.

Αυτή η υποχρέωση αναφοράς στην εποπτική αρχή και ενδεχομένως και στα υποκείμενα των δικαιωμάτων, ατομικά ή με ανακοίνωση, όπως κρίνεται κατάλληλο κάθε φορά, υπάρχει στον ΓΚΠΔ, για να μπορέσουν να λάβουν μέτρα για τον περιορισμό των αρνητικών συνεπειών των παραβιάσεων. Η υποχρέωση ενημέρωσης προς τα φυσικά πρόσωπα υπάρχει όταν η παραβίαση δεδομένων ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους[67]. Οι υπεύθυνοι επεξεργασίας οφείλουν να γνωστοποιούν ορισμένες παραβιάσεις δεδομένων στις εποπτικές αρχές αμελλητί και, εάν είναι εφικτό, εντός 72 ωρών από τη στιγμή που έλαβαν γνώση της παραβίασης. Από την υποχρέωσή τους αυτή απαλλάσσονται, μόνο όταν είναι σε θέση να αποδείξουν ότι η παραβίαση των δεδομένων δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των ενδιαφερόμενων φυσικών προσώπων και όταν έχουν υιοθετηθεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και ιδίως αυτό της κρυπτογράφησης.

Παρόμοια διάταξη υπάρχει και στο πλαίσιο της Εκσυγχρονισμένης Σύμβασης 108 του Συμβουλίου της Ευρώπης, τα συμβαλλόμενα μέρη οφείλουν, τουλάχιστον, να υποχρεώνουν τους υπευθύνους επεξεργασίας να γνωστοποιούν στην αρμόδια εποπτική αρχή παραβιάσεις δεδομένων οι οποίες ενδέχεται να συνιστούν σοβαρή επέμβαση στα δικαιώματα των υποκειμένων των δεδομένων. Η γνωστοποίηση αυτή θα πρέπει να πραγματοποιείται «αμελλητί»[68].

Αντίστοιχη υποχρέωση υπάρχει και στους εκτελούντες την επεξεργασία και για το λόγο αυτό θα πρέπει να διασφαλίζεται ότι και αυτοί υποχρεούνται να αναφέρουν τις

[66] Ό.π. Ομάδα εργασίας του άρθρου 29, WP250rev.01, σελ. 6

[67] Ό.π., άρθρο 34 ΓΚΠΔ

[68] Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 2· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημεία 64-66

παραβιάσεις δεδομένων. Αυτοί αντίστοιχα έχουν υποχρέωση να αναφέρουν τις παραβιάσεις δεδομένων στο υπεύθυνο επεξεργασίας[69]. Σύμφωνα επίσης με τις ανανεωμένες κατευθυντήριες γραμμές[70] «ο εκτελών την επεξεργασία πρέπει απλώς να διαπιστώσει εάν έχει σημειωθεί παραβίαση και στη συνέχεια να ειδοποιήσει τον υπεύθυνο επεξεργασίας. Ο υπεύθυνος επεξεργασίας χρησιμοποιεί τον εκτελούντα την επεξεργασία για να επιτύχει τους σκοπούς του: συνεπώς, κατ' αρχήν, ο υπεύθυνος επεξεργασίας πρέπει να θεωρείται ότι αποκτά «γνώση» τη στιγμή που ο εκτελών τον ενημερώσει σχετικά με την παραβίαση». Η νέα αυτή διατύπωση, έχει σημαντικές επιπτώσεις σε σχέση με το χρονικό σημείο από όπου αρχίζουν να υπολογίζεται η προθεσμία των 72 ωρών για τη γνωστοποίηση στην εποπτική αρχή.

4.5.1 Κριτήρια αξιολόγησης κινδύνου παραβίασης

Υψηλός κίνδυνος θεωρείται ότι υφίσταται όταν η παραβίαση ενδέχεται να οδηγήσει σε σωματική, υλική ή ηθική βλάβη για τα πρόσωπα τα δεδομένων των οποίων έχουν παραβιαστεί. Τέτοια βλάβη μπορεί να αποτελέσουν διακρίσεις, καταχρήσεις ταυτότητας, οικονομική απώλεια ή βλάβη φήμης[71]. Όταν η παραβίαση αφορά δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών, τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα ή περιλαμβάνει δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας, αυτή η βλάβη θα πρέπει να θεωρείται πιθανό να επέλθει[72]. Όσο μεγαλύτερος είναι ο βαθμός ευαισθησίας των δεδομένων, τόσο υψηλότερος είναι και ο κίνδυνος βλάβης για τα επηρεαζόμενα πρόσωπα, χωρίς να αποκλείεται να επέλθει όμως σοβαρή βλάβη από την αποκάλυψη ακόμα και απλών δεδομένων προσωπικού χαρακτήρα, όταν λχ. η ταυτοποίηση ενός προσώπου ή η αποκάλυψη σχέσεων με τρίτους μπορούν να επιφέρουν σοβαρότατη βλάβη στα υποκείμενα ή σε τρίτους. Κατά την αξιολόγηση του κινδύνου, ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει τις ειδικές περιστάσεις της παραβίασης, συμπεριλαμβανομένων της σοβαρότητας του πιθανού αντίκτυπου και της πιθανότητας να

[69] Ό.π., άρθρο 33 παράγραφος 2

[70] Ό.π. Ομάδα εργασίας του άρθρου 29, WP250rev.01, σελ. 16

[71] Ομάδα εργασίας του άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP250rev.01, 3 Οκτωβρίου 2017, σελ. 27

[72] Βλ. αιτιολογικές σκέψεις 75 και 85 ΓΚΠΔ

προκύψει -όπως και να λαμβάνεται υπόψη η πιθανότητα και η σοβαρότητα του κινδύνου αυτής- βάσει αντικειμενικής εκτίμησης[73].

Στο πλαίσιο μιας ΕΑΠΔ, η αξιολόγηση του κινδύνου για τα δικαιώματα και τις ελευθερίες των προσώπων ως αποτέλεσμα μιας παραβίασης, είναι διαφορετική[74] καθώς εξετάζονται τόσο οι κίνδυνοι της επεξεργασίας των δεδομένων που πραγματοποιείται όπως έχει προβλεφθεί, όσο και οι κίνδυνοι σε περίπτωση παραβίασης. Η αξιολόγηση αυτή είναι υποθετική, αφού γίνεται για ενδεχόμενα μελλοντικά συμβάντα, σε αντίθεση με τα περιστατικά πραγματικής παραβίασης, όπου το συμβάν έχει ήδη προκύψει και συνεπώς σε αυτή τη περίπτωση η προσοχή εστιάζεται αποκλειστικά στον κίνδυνο που απορρέει από τις συνέπειες της παραβίασης για τα πρόσωπα.

Η Ομάδα εργασίας του άρθρου 29 συνιστά -κατά την αξιολόγηση- να λαμβάνονται ως κριτήρια[75] το είδος της παραβίασης, η φύση, η ευαισθησία και ο όγκος των δεδομένων προσωπικού χαρακτήρα, η ευκολία ταυτοποίησης των προσώπων, η σοβαρότητα των συνεπειών για τα πρόσωπα και το αν ελλοχεύει κίνδυνος μεγαλύτερης βλάβης για κάποιους, τα ειδικά χαρακτηριστικά του προσώπου (ανηλικότητα ή ευάλωτα άτομα), τα ειδικά χαρακτηριστικά του υπευθύνου επεξεργασίας δεδομένων, σε περίπτωση που η φύση και ο ρόλος τους επηρεάζουν το επίπεδο κινδύνου και τον αριθμό των επηρεαζόμενων προσώπων.

4.5.2 Η περίπτωση της ανωνυμοποίησης ως λόγος εξαίρεσης από την υποχρέωση γνωστοποίησης

Η ανωνυμοποίηση των δεδομένων δύναται να αποτελέσει και αυτή ένα λόγο εξαίρεσης από την υποχρέωση γνωστοποίησης όταν χρησιμοποιείται για την προστασία των προσωπικών δεδομένων από τους υπεύθυνους επεξεργασίας[76]. Ο Κανονισμός

[73] Βλ. αιτιολογικές σκέψεις 75 και 76 ΓΚΠΔ

[74] Βλ. κατευθυντήριες γραμμές της Ομάδας εργασίας του άρθρου 29 για τις ΕΑΠΔ: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (τελευταία πρόσβαση 9-2-2021)

[75] Το άρθρο 3.2 του Κανονισμού (ΕΕ) 611/2013 παρέχει καθοδήγηση όσον αφορά τους παράγοντες που θα πρέπει να λαμβάνονται υπόψη σε σχέση με την κοινοποίηση παραβιάσεων στον τομέα των υπηρεσιών ηλεκτρονικών επικοινωνιών, η οποία μπορεί να είναι χρήσιμη στο πλαίσιο της γνωστοποίησης δυνάμει του ΓΚΠΔ
Βλ. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:el:PDF (τελευταία πρόσβαση 9-2-2021)

[76] Σύμφωνα με την άποψη της ομάδας εργασίας του άρθρου 29 όσον αφορά την υποχρέωση αναφοράς, υπάρχουν τρία διακριτά είδη παραβιάσεων προσωπικών δεδομένων: 1. Παραβίαση διαθεσιμότητας, όπως η τυχαία ή παράνομη καταστροφή δεδομένων, 2. Παραβίαση ακεραιότητας, η οποία συντελείται με τροποποίηση δεδομένων και 3. Παραβίαση εμπιστευτικότητας μέσω της μη εξουσιοδοτημένης πρόσβασης

611/2013 στα εφαρμοζόμενα μέτρα ενημέρωσης των υποκειμένων σε περιπτώσεις παραβίασης δεδομένων υπό την Οδηγία (ΕΕ) 2002/58 αναφέρει ότι «η κοινοποίηση παραβίασης προσωπικών δεδομένων σε ενδιαφερόμενο συνδρομητή ή άτομο δεν απαιτείται, εάν ο πάροχος έχει αποδείξει κατά ικανοποιητικό τρόπο για την αρμόδια αρχή ότι έχει εφαρμόσει κατάλληλα τεχνολογικά μέτρα προστασίας και ότι τα μέτρα αυτά εφαρμόστηκαν ως προς τα δεδομένα που αφορούσε η παραβίαση της ασφάλειας. Τα εν λόγω τεχνολογικά μέτρα προστασίας πρέπει να καθιστούν τα δεδομένα ακατανόητα σε οποιοδήποτε πρόσωπο δεν διαθέτει δικαίωμα πρόσβασης σε αυτά»[77]. Αποδεκτά μέτρα που μπορεί να θεωρηθούν ότι τα δεδομένα «μη κατανοητά» είναι (1) όταν έχουν κρυπτογραφηθεί με τυποποιημένο αλγόριθμο, το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων δεν έχει παραβιαστεί σε οποιαδήποτε παραβίαση της ασφάλειας, και το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων έχει δημιουργηθεί κατά τρόπο, που να μην μπορεί να εξακριβωθεί με τα διαθέσιμα τεχνολογικά μέσα από οποιοδήποτε πρόσωπο που δεν έχει εξουσιοδοτημένη πρόσβαση στο κλειδί ή (2) έχουν αντικατασταθεί από την τιμή κατακερματισμού τους, που έχει υπολογιστεί με τυποποιημένη κρυπτογράφηση συνάρτησης κατακερματισμού και τηρούνται οι ίδιες προϋποθέσεις ασφάλειας όπως στην πρώτη παράγραφο[78].

Παρόλα αυτά, ανεξαρτήτως των τεχνολογικών μέτρων που εφαρμόζονται, οι οργανισμοί ακόμα και να εξαιρεθούν από την υποχρέωση ανακοίνωσης στα υποκείμενα των δικαιωμάτων, συνεχίζουν να έχουν υποχρέωση ανακοίνωσης στην αρμόδια εποπτεύουσα Αρχή[79]. Παρομοίως και στον ΓΚΠΔ, ορίζεται στο άρθρο 34, ότι η ανακοίνωση δεν απαιτείται στο υποκείμενο των δικαιωμάτων αν διαζευκτικά (1) ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας και τα δεδομένα είναι ανωνυμοποιημένα ή (2) έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος ή (3) προϋποθέτει δυσανάλογες προσπάθειες[80].

σε προσωπικά δεδομένα (Opinion 03/2014 on Personal Data Breach Notification, WP 213, 25 Μαρτίου 2014, σελ.2). Βλ. επίσης σημείωση για «μη κατανοητά δεδομένα» στον κανονισμό 611/2013, τα οποία δεν αποτελούν παραβίαση διαθεσιμότητας και ενδεχομένως να απαλλάσσουν την οντότητα από την υποχρέωση ενημέρωσης, βλ. A.Tamo-Larrieux p. 209, και εκεί παραπομπές ιδίως Esayas, p. 14.

[77] Άρθρο 4 παρ. 1 Κανονισμού 611/2013

[78] Άρθρο 4 παρ. $2^{\alpha, \beta}$ Κανονισμού 611/2013

[79] Βλ. Esayas, p. 14.

[80] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 34 παράγραφος 2 ΓΚΠΔ

5 ΑΣΦΑΛΗΣ ΣΧΕΔΙΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

5.1 Ασφάλεια πληροφοριών

Η Ασφάλεια Πληροφοριών (Information Security) έχει ως σκοπό την προστασία των συστατικών ενός πληροφοριακού συστήματος από πιθανές επιπτώσεις στην εμπιστευτικότητα και την ακεραιότητά τους, αλλά και την εξασφάλιση της διαθεσιμότητάς τους προς τους εξουσιοδοτημένους χρήστες. Προς αυτή την κατεύθυνση, η λήψη των κατάλληλων μέτρων προστασίας μπορεί να αφορά μια ή περισσότερες από τις ακόλουθες τρεις φάσεις:

- Πρόληψη (prevention) περιστατικών ασφάλειας σε συστατικά του πληροφοριακού συστήματος (π.χ. κλείδωμα φυσικών χώρων, κρυπτογράφηση, κα.),
- Ανίχνευση (detection) περιστατικών ασφάλειας είτε πριν είτε κατά τα διάρκεια είτε μετά την πραγματοποίησή τους σε συστατικά του πληροφοριακού συστήματος (π.χ. κύκλωμα με κάμερες, αρχεία καταγραφής – log files).
- Αντίδραση (reaction) σε περιστατικά ασφάλειας είτε για την έγκαιρη αντιμετώπισή τους είτε για την ανάκτηση των συστατικών του πληροφοριακού συστήματος που δέχθηκαν πλήγμα[81] (π.χ. κλήση αστυνομίας, επαναφορά αρχείων από backup).

Η Ασφάλεια Πληροφοριών αφορά την προστασία των ακόλουθων τριών θεμελιωδών ιδιοτήτων:

- Εμπιστευτικότητα (confidentiality). Αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη αποκάλυψή (ανάγνωσή) της. Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Ακεραιότητα (integrity): αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη μεταβολή (τροποποίηση ή διαγραφή) της. Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
- Διαθεσιμότητα (availability): αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης (είτε για ανάγνωση είτε για τροποποίηση) στην πληροφορία, χωρίς

[81] Ασφάλεια Πληροφοριών στο Διαδίκτυο, Ι.Μαυρίδης, 2005

εμπόδια ή καθυστέρηση. Τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Πλήγμα σε οποιοδήποτε από τα ανωτέρω, από τυχαία ή εσκεμμένη ενέργεια, συνιστά γενικά, περιστατικό ασφάλειας.

Εκτός από τις παραπάνω βασικές ιδιότητες, η ασφάλεια των πληροφοριών συσχετίζεται με την επιτυχημένη εφαρμογή των ακόλουθων μηχανισμών:

- Αναγνώρισης (Identification): αφορά τη διαδικασία παρουσίασης της ταυτότητας μιας οντότητας (π.χ. τελικοί χρήστες, άλλες υπηρεσίες, διαδικασίες, ή υπολογιστές) στο σύστημα.
- Αυθεντικοποίησης (Authentication): αφορά τη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα.
- Εξουσιοδότησης (Authorization): αφορά τη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μιας αυθεντικοποιημένης οντότητας στο σύστημα, στη βάση των δικαιωμάτων πρόσβασης που της έχουν ήδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος.
- Αδυναμία αποποίησης (Non-Repudiation): αφορά τη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μιας ενέργειας στο σύστημα. Αποτελείται από ένα σύστημα επιθεώρησης και καταγραφής που μπορεί να είναι το κλειδί για μια υπηρεσία αδυναμίας αποποίησης. Μια τέτοια υπηρεσία εγγυάται ότι ο πελάτης δεν μπορεί να αρνηθεί την ευθύνη για την εκτέλεση μιας ενέργειας από μέρους του (π.χ. μιας ηλεκτρονικής συνδιαλλαγής)[82].

Ως Πληροφοριακό Σύστημα[83] εννοούμε το οργανωμένο σύνολο από ανθρώπους, λογισμικό, υλικό, διαδικασίες, εγκαταστάσεις και δεδομένα και την εσωτερική αλληλεπίδρασή τους. Οι σύγχρονοι οργανισμοί εξαρτώνται από την διαχείριση των πληροφοριών ως αγαθά, καθώς από αυτά εξαρτάται η εύρυθμη λειτουργία τους. Η υλοποίηση της διαδικασίας προστασίας του πληροφοριακού αυτού αγαθού εξαρτάται από πολλούς παράγοντες μέσα σε κάθε οργανισμό. Στοιχειώδης αρχή είναι η κατάρτιση πολιτικών ασφάλειας πληροφοριών και ο καθορισμός των στόχων και των

[82] Ι.Μαυρίδης, ο.π, σελ. 90
[83] Ι.Μαυρίδης, ο.π., σελ. 208

δραστηριοτήτων του κάθε οργανισμού και των εργαζομένων του. Ανεξαρτήτως ποια λύση προσφέρει την μέγιστη προστασία για τον κάθε οργανισμό, θα πρέπει κατανοηθούν οι απαιτήσεις ασφαλείας με ορθή αποτίμηση της επικινδυνότητας και να υπάρχει μια ξεκάθαρη προσέγγιση και ένα πλάνο υλοποίησης και επίβλεψης, συμβατό με την κουλτούρα του κάθε οργανισμού, ώστε να μειώνεται ο χρόνος εφαρμογής και να αυξάνεται το επίπεδο ενσωμάτωσης των αλλαγών. Σημαντικό προς το σκοπό αυτό είναι επίσης να υπάρχουν οι ανάλογοι οικονομικοί πόροι, επαρκής ευαισθητοποίηση και εκπαίδευση των μερών του οργανισμού και αφού ολοκληρωθεί η δημιουργία συστήματος αξιολόγησης της ασφάλειας των πληροφοριών, ώστε να δημιουργηθούν οι διαδικασίες αρχικά και να προτείνονται βελτιώσεις έπειτα.

Η ανάπτυξη μιας τακτικής για την ασφάλεια πληροφοριών σε κάθε οργανισμό, απαιτεί τον συντονισμό ειδικών διαφόρων ειδικοτήτων, καθώς απαιτούνται γνώσεις πληροφορικής, νομικού πλαισίου και διοικητικής μέριμνας ώστε να μπορούν να εφαρμοστούν οι απαιτούμενες διαδικασίες ως σύνολο. Η διαδικασία αυτή περιλαμβάνει την δημιουργία επιμέρους πολιτικών αλλά και εναρμόνιση με διεθνείς πρακτικές και πρότυπα ώστε να παίρνονται σωστές αποφάσεις από τις διοικήσεις των οργανισμών αλλά να είναι δυνατή η αξιολόγηση των συστημάτων διαχείρισης ασφάλειας πληροφοριών.

Το σημαντικότερο ζήτημα στα σύγχρονα πληροφοριακά συστήματα, είναι αυτό της διαχείρισης της ασφάλειας πληροφοριών, καθώς από αυτή εξαρτάται η αξιοπιστία ενός συστήματος. Η χρησιμοποίηση επιπλέον νέων τεχνολογιών (SaaS, Blockchain) προσφέρει μεν περισσότερες δυνατότητες αλλά αυξάνει αναλογικά και τα προβλήματα στην ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριακών αγαθών. Προς εξασφάλιση αυτών είναι απαραίτητη η δημιουργία ασφαλών πολιτικών -βάσει των οποίων- θα είναι δυνατός ο εντοπισμός και χαρακτηρισμός των ευαίσθητων δεδομένων των οποίων η επεξεργασία, η μεταφορά και η αποθήκευση πρέπει να προστατεύεται.

5.2 Διαφάνεια

5.2.1 Η απεικόνιση ως μέσο διαφάνειας

Η απαίτηση για διαφάνεια επεξεργασίας είναι μέρος της γενικής απαίτησης για νομιμότητα και ορθότητα στην επεξεργασία και ενσωματώνεται στα άρθρα 12, 13, 14 και 34 του ΓΚΠΔ, όπως προαναφέρθηκε. Ο ΓΚΠΔ αναγνωρίζει την σημαντικότητα της απεικόνισης ως μέσο ενίσχυσης της αρχής της διαφάνειας. Στην αιτιολογική σκέψη (58),

ορίζεται ότι η αρχή της διαφάνειας απαιτεί «οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή». Επίσης, ορίζεται ότι πρέπει «να χρησιμοποιείται σαφής και απλή διατύπωση και, επιπλέον, κατά περίπτωση, απεικόνιση». Η απαίτηση αυτή είναι κρίσιμη όταν είναι ιδιαίτερα δύσκολο για τα υποκείμενα να αντιληφθούν ότι συλλέγονται προσωπικά τους δεδομένα, από ποιόν και για ποιο σκοπό[84]. Όταν μάλιστα τα προσωπικά δεδομένα αφορούν παιδιά, οι ενημερώσεις μέσω της απεικόνισης πρέπει να είναι σε μορφή που να μπορούν να αντιληφθούν. Παρά το ότι δεν παρέχονται αναλυτικές οδηγίες για τον τρόπο ενσωμάτωσης στο σχεδιασμό της απαίτησης για απεικόνιση, αυτή μπορεί να γίνει με τρόπο αποτελεσματικό μέσω της εκτίμησης αντικτύπου.

Η εφαρμογή της απαίτησης για απεικόνιση των ενημερώσεων, γίνεται και στην περίπτωση χρησιμοποίησης συστημάτων βιντεοεπιτήρησης, όπου οι υπεύθυνοι επεξεργασίας οφείλουν να παρέχουν πλήρη ενημέρωση για τη λειτουργία καμερών, πριν κάποιος εισέλθει στον επιτηρούμενο χώρο. Για τον σκοπό αυτό προτείνεται από τις Κατευθυντήριες γραμμές 3/2019 του ΕΣΠΔ[85] και την ΑΠΔΠΧ με τις συστάσεις 2/2020[86] να ακολουθείται πολυεπίπεδη προσέγγιση, η οποία προτείνει να υπάρχουν ενημερωτικές πινακίδες για την άμεση ενημέρωση όσων εισέρχονται στο χώρο (πληροφορίες Α' επιπέδου), οι οποίες να παραπέμπουν σε εύκολα προσβάσιμη αναλυτική ενημέρωση (πληροφορίες Β' επιπέδου), ώστε να υπάρχει πλήρης διαφάνεια ως προς τον τρόπο, τους σκοπούς επεξεργασίας και την ταυτότητα του υπευθύνου επεξεργασίας και έπειτα εφόσον το υποκείμενο το επιθυμεί ως προς τα δικαιώματά του.

5.2.2 Εκτίμηση αντικτύπου

Η αποτίμηση των επιπτώσεων ενός πληροφοριακού συστήματος ή μιας επεξεργασίας στην ιδιωτικότητα, η λεγόμενη Data Protection Impact Assessment (DPIA)[87], είναι το βασικό εργαλείο με σκοπό να αξιολογηθεί εάν οι σχεδιαστικές επιλογές

[84] Αιτιολογική σκέψη, υπ' αριθμ. 58 ΓΚΠΔ.

[85] Κατευθυντήριες γραμμές 3/2019 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω βιντεοσυσκευών του Ευρωπαϊκού Συμβούλιο Προστασίας Δεδομένων, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_el (τελευταία πρόσβαση 1-2-2021).

[86] Συστάσεις υπ' αριθμ. 2/2020 της ΑΠΔΠΧ, https://www.dpa.gr/sites/default/files/2020-12/Sistaseis_2_2020.pdf (τελευταία πρόσβαση 1-2-2021).

[87] Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, ό.π., σελ. 100 επ· Λ. Μήτρου, Privacy by Design Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔΙΤΕ (π. ΔΙΜΕΕ),

για ένα σύστημα ή μία διαδικασία, αντιστοιχούν στις απαιτήσεις για τη διασφάλιση της ιδιωτικότητας. Αποτελεί μια συστηματική διαδικασία για την αξιολόγηση των ενδεχόμενων κινδύνων για την προστασία δεδομένων των φυσικών προσώπων όσον αφορά ένα σχεδιαζόμενο σύστημα επεξεργασίας δεδομένων και την εύρεση τρόπων μετριασμού των κινδύνων ή πρόληψης αρνητικών συνεπειών[88].

Στον ΓΚΠΔ η απαίτηση για εκτίμηση αντικτύπου ενσωματώνεται στο άρθρο 35, το οποίο τελεί σε στενή σχέση με το άρθρο 25 για ασφάλεια εκ του σχεδιασμού. Η πρώτη παράγραφος του άρθρου 25 ορίζει ότι «ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας», με αυτό τον τρόπο υιοθετείται μια προσέγγιση προστασίας ανά επεξεργασία, όπως γίνεται και στις εκτιμήσεις κινδύνου[89].

Με βάση τον ΓΚΠΔ επίσης, η εκτίμηση αντικτύπου είναι υποχρεωτική[90], όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η υποχρεωτικότητά της, στις ορισμένες αυτές περιπτώσεις επιβλήθηκε λόγω και της κατάργησης της υποχρέωσης γνωστοποίησης στην εποπτική αρχή της επεξεργασίας και προηγούμενου ελέγχου των επεξεργασιών που ενέχουν ειδικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[91].

Ο σκοπός της εκτίμησης αντικτύπου είναι να διασφαλιστεί η συμμόρφωση με τις απαιτήσεις του Νόμου, αποτελώντας κομμάτι του συνολικού ασφαλούς σχεδιασμού. Εφαρμόζεται ήδη πριν από το στάδιο του σχεδιασμού ενός συστήματος ή μιας επεξεργασίας και δεν αποτελεί απλώς έναν έλεγχο συμμόρφωσης του οργανισμού προς

τεύχος 1/2013, κεφ. «Αξιολόγηση επιπτώσεων στην ιδιωτικότητα και εξ ορισμού ιδιωτικότητα» και Γνώμες 5/2010 και 11/2011 Ομάδας του άρθρου 29 Working Party (WP29) σχετικά με την πρόταση του κλάδου για αποτίμηση των επιπτώσεων της αναγνώρισης ταυτότητας μέσω ραδιοσυχνοτήτων.

[88] 3 Βλ. D. Wright, Should Privacy Impact Assessments Be Mandatory?, Communications of the ACM, July 2011, vol. 54, No. 8, σελ. 121 επ. (123).

[89] Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework και παραπομπές στα πρότυπα NIST Risk Management Guide, 2002 or the ISO/IEC 27005: 2011, p. 182

[90] Η μη συμμόρφωση με την υποχρέωση διενέργειας εκτίμησης αντικτύπου επιφέρει συνέπειες, δηλ. διοικητικά πρόστιμα και αποζημίωση, βλ. σχετ. Ιγγλεζάκη, Ο Γενικός Κανονισμός προστασίας Προσωπικών Δεδομένων, (γ΄εκδ.) 2020, σελ. 256. Επίσης, βλ. https://www.dpa.gr/portal/page?_pageid=33,223264&_dad=portal&_schema=PORTAL (τελευταία πρόσβαση 5-2-2021)

[91] Βλ. Ι. Ιγγλεζάκη, Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων, Τομ. 1, τεύχ. 1 (2020), Κεφ.ΙΙ

την νομοθεσία, αλλά συνιστά μια ενδελεχή αξιολόγηση των τεχνολογικών προτάσεων, σκοπών και μέσων της κάθε επεξεργασίας, κρίνοντας την αναγκαιότητα την εφαρμογής του μέτρου με βάση την αρχή της αναλογικότητας. Συμπεριλαμβάνει επίσης έκθεση των κινδύνων που εμπεριέχει η κάθε σκοπούμενη επεξεργασία και ανάλυση των εγγυήσεων που προβλέπονται.

5.2.3 Πιστοποιήσεις ασφαλείας

Στο άρθρο 42 του ΓΚΠΔ υπάρχει παρότρυνση για «τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων», εφαρμόζοντας την αρχή της ασφάλειας εκ του σχεδιασμού και εξ ορισμού. Ο ΓΚΠΔ, αντίθετα με την Οδηγία 95/46/ΕC, αναλύει την απαίτηση για πιστοποίηση και σφραγίδων. Η πιστοποίηση τήρηση επιπέδων ασφάλειας αποδεικνύουν ότι πληρούνται κατ' ελάχιστο κάποια επίπεδα ασφαλείας, παρέχοντας έτσι στους υπευθύνους επεξεργασίας μεγαλύτερη ασφάλεια δικαίου.

Η αιτιολογική σκέψη 100 του ΓΚΠΔ, αναφέρει ευθέως ως τρόπο βελτίωσης της συμμόρφωσης και αύξηση της διαφάνειας, την «θέσπιση μηχανισμών πιστοποίησης και σφραγίδων και σημάτων προστασίας των δεδομένων», με την οποία επιτυγχάνεται ευθεία αξιολόγηση σχετικών προϊόντων και υπηρεσιών από τα υποκείμενα των δεδομένων. Όπως επίσης και το άρθρο 42 του ΓΚΠΔ, ενθαρρύνει την ευθεία υιοθέτηση πανευρωπαϊκών προτύπων[92] προς εξασφάλιση της διαφάνειας.

Παρακάτω θα αναλυθούν τα πιο διαδεδομένα πρότυπα, προς εξασφάλιση μεγαλύτερου επιπέδου διαφάνειας σε υπηρεσίες και προϊόντα αλλά και ασφάλειας κατά την διαβίβαση δεδομένων.

5.2.3.1 TRUSTe και EuroPriSe

Τα δύο πρότυπα TRUSTe και EuroPriSe παρέχουν στους υπευθύνους επεξεργασίας κανόνες και περιορισμούς για τη σωστή τήρηση των οποίων μπορούν να λάβουν σχετική πιστοποίηση για τον οργανισμό τους. Τα πρότυπα αυτά βασίζονται σε όλη

[92] Βλ. παρ.1 άρθρου 42 ΓΚΠΔ «Τα κράτη μέλη, οι εποπτικές αρχές, το Συμβούλιο Προστασίας Δεδομένων και η Επιτροπή παροτρύνουν, ιδίως σε ενωσιακό επίπεδο, τη θέσπιση μηχανισμών πιστοποίησης προστασίας δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων, με σκοπό την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Λαμβάνονται υπόψη οι ειδικές ανάγκες των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων».

την Ευρωπαϊκή Νομοθεσία περί προστασίας προσωπικών δεδομένων όπως και άλλα υπάρχοντα πλαίσια[93].

Το πρότυπο TRUSTe[94], απαιτεί από τον υπεύθυνο επεξεργασίας να υποβάλλει μια δήλωση προκειμένου να πάρει το πιστοποιητικό. Η δήλωση αυτή πρέπει να είναι εύκολα προσβάσιμη από τα υποκείμενα των δεδομένων και να περιέχει αναλυτικά τις πληροφορίες που συλλέγονται, εάν και σε ποιόν διαβιβάζονται, καθώς και πως μπορούν να ασκηθούν τα δικαιώματα πρόσβασης, ανάκλησης της συναίνεσης ή το δικαίωμα στην λήθη. Παράλληλα, επιβάλλονται διάφοροι περιορισμοί στην επεξεργασία των δεδομένων, όπως ενδεικτικά απαιτείται η ύπαρξη συστημάτων τήρησης της αρχής του περιορισμού του σκοπού κ.α.

Η EuroPriSe στηρίχθηκε στην Οδηγία 95/46/EC αλλά συνεχίζει να εφαρμόζεται και μετά τον ΓΚΠΔ καθώς τα κριτήριά της ενημερώθηκαν[95]. Τα κριτήρια παρέχουν έναν κατάλογο ερωτημάτων, σε κατηγορίες βάσει των αρχών προστασίας προσωπικών δεδομένων, με τα οποία μπορεί να διαπιστωθεί αν κάποιο προϊόν ή υπηρεσία παρέχει το απαιτούμενο επίπεδο ασφαλείας.

Οι πιστοποιήσεις και οι σφραγίδες προστασίας ιδιωτικότητας στοχεύουν στην παροχή επαρκούς επιπέδου ασφαλείας και στη συμμόρφωση των υπευθύνων επεξεργασίας. Βεβαιώνουν ουσιαστικά ότι το επίπεδο ασφαλείας που ισχυρίζεται ο υπεύθυνος επεξεργασίας ότι το τηρεί, ανταποκρίνεται στην πραγματικότητα, παίζοντας το ρόλο «αρχής», δρώντας ως ανεξάρτητο ίδρυμα..

5.2.3.2 Privacy Shield και απόφαση C-311/18 του ΔΕΕ στην υπόθεση «Schrems II»

Το Privacy Shield[96] αποτελούσε ένα μηχανισμό αυτοπιστοποίησης για εταιρείες που εδρεύουν στις ΗΠΑ. Είχε αναγνωριστεί με Εκτελεστική Απόφαση της Ευρωπαϊκής

[93] Βλ. ενδεικτικά το πλαίσιο προστασίας της ιδιωτικότητας του Οργανισμού OECD, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, (τελευταία πρόσβαση 3-2-2021)

[94] Το πρότυπο TRUSTe LLC (TRUSTe), αποτελεί μέρος του TrustArc, και έχει βασιστεί στα: GDPR, ISO 27001, U.S. Health Insurance Portability and Accountability Act (HIPAA), OECD Privacy Guidelines και APEC Privacy Framework, βλ. σχετικά https://trustarc.com/consumer-info/privacy-certification-standards/, (τελευταία πρόσβαση 3-2-2021)

[95] Βλ. Κριτήρια EuroPriSe: https://www.euprivacyseal.com/EPS-en/Criteria, (τελευταία πρόσβαση 3-2-2021)

[96] Βλ. Ι. Ιγγλεζάκη, Ι., Η ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα (EU-US Privacy Shield), Συνήγορος 113/2016, σελ. 68 επ.

Επιτροπής (ΕΕ) 2016/1250 ότι εξασφαλίζει ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων που διαβιβάζονται από οργανισμούς της ΕΕ σε οργανισμούς οι οποίοι έχουν αυτοπιστοποιηθεί ότι παρέχουν τις κατάλληλες νομικές εγγυήσεις για αυτές τις διαβιβάσεις δεδομένων και δεσμεύονται να τηρούν ένα σύνολο αρχών προστασίας της ιδιωτικής ζωής — τις λεγόμενες αρχές του πλαισίου της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ.

Στις 16 Ιουλίου του 2020, το Δικαστήριο της ΕΕ (ΔΕΕ) εξέδωσε απόφαση[97], με βάση την οποία καταργείται το Privacy Shield, το νομικό εργαλείο δηλαδή που καθιστούσε ελεύθερη την διαβίβαση προσωπικών δεδομένων στις ΗΠΑ. Ταυτόχρονα όμως, έκρινε ότι παραμένουν σε ισχύ οι Τυποποιημένες Συμβατικές Ρήτρες (ΤΣΡ), ένα άλλο νομικό εργαλείο που μπορεί να χρησιμοποιηθεί για διαβίβαση δεδομένων σε τρίτες χώρες, με αυστηρές όμως προϋποθέσεις. Η απόφαση αυτή επηρεάζει όλους τους οργανισμούς που διαβιβάζουν ή προτίθενται να διαβιβάσουν δεδομένα σε τρίτες χώρες και ιδιαίτερα στις ΗΠΑ[98].

Το ΔΕΕ, αφού εξέτασε διάφορους παράγοντες και ιδιαίτερα το νομικό καθεστώς των ΗΠΑ που αφορά στην παρακολούθηση δεδομένων από την ΕΕ στις ΗΠΑ, κήρυξε ανίσχυρο το Privacy Shield.

Συγκεκριμένα, η σημαντικότερη διαπίστωση που έγινε από το δικαστήριο και βάσει της οποίας αποφάσισε στην υπόθεση "Schrems II", ήταν το ότι οι ισχύοντες Νόμοι στην Αμερική, επέτρεπαν την παρακολούθηση πέραν των ορίων που επιτρέπει ο ΓΔΚΠ και ότι παρέχονταν ανεπαρκή ένδικα μέσα ενάντια στην Κυβέρνηση σε περίπτωση διαπιστωθείσας παραβίασης δεδομένων από αυτήν. Το ΔΕΕ αιτιολόγησε την απόφαση

---

[97] Η υπόθεση C-311/18 «Data Protection Commissioner of Ireland v. Facebook & Max Schrems» («Schrems II») του Δικαστηρίου της Ευρωπαϊκής Ένωσης έθεσε ως επίκεντρο το προδικαστικό ερώτημα που υπεβλήθη, το Μάιο του 2018, από το Ανώτερο Δικαστήριο της Ιρλανδίας ενώπιον του ΔΕΕ, σχετικά με την προσφυγή της Ιρλανδικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ενάντια στο Facebook και τον Max Schrems. Ειδικότερα, αφορά στην καταγγελία που υπέβαλε ο τελευταίος ενώπιον της Ιρλανδικής Αρχής με σκοπό την απαγόρευση διαβίβασης των προσωπικών του δεδομένων βάσει των τυποποιημένων συμβατικών ρητρών προστασίας δεδομένων, οι οποίες περιλαμβάνονταν στο παράρτημα της σχετικής απόφασης της Ευρωπαϊκής Επιτροπής (Τυποποιημένες Συμβατικές Ρήτρες), βλ. http://curia.europa.eu/juris/document/document.jsf;jsessionid=699F5010F9ED77A76EF28523A1A60EE9?text=&docid=228677&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=10320201 (τελευταία πρόσβαση 12-2-2021)

[98] βλ. και Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων), ΔΙΤΕ (π. ΔΙΜΕΕ), Τεύχος 1/2016

λέγοντας ότι η δέσμευση της εταιρείας να επεξεργάζεται τα δεδομένα με ασφάλεια ήταν ανώφελη από την στιγμή που δεν μπορεί να εμποδίσει την Κυβέρνηση απ' το να παρακολουθεί τα προσωπικά δεδομένα ούτε και γίνεται να εξασφαλίσουν, μέσω συμβάσεων, την δυνατότητα προσφυγής στη δικαιοσύνη στην περίπτωση που η Κυβέρνηση παραβιάσει δεδομένα. Συνεπώς, οι δεσμεύσεις που γινόντουσαν υπό το Privacy Shield, δεν μπορούσαν να παρέχουν επαρκές επίπεδο ασφάλειας των προσωπικών δεδομένων.

Η ίδια λογική ισχύει και στις ΤΣΡ, οι ιδιώτες δεν μπορούν να συμβληθούν παρακάμπτοντας τους νόμους που επιτρέπουν την επιτήρηση.

Η έκδοση αυτής της απόφασης είχε ως αποτέλεσμα πολλές Αρχές Προσωπικών Δεδομένων στην Ευρώπη να απαγορεύσουν μερικώς ή και εντελώς αρχικά διαβιβάσεις δεδομένων στην Αμερική με βάση τις ΤΣΡ.

Το ΕΣΠΔ παρότι στην αρχή δήλωσε ότι ίσως οι ΤΣΡ δεν επαρκούν για να εξασφαλίσουν το απαιτούμενο επίπεδο προστασίας, διευκρίνισε έπειτα, μέσω συστάσεων, ότι ίσως είναι επαρκείς, εφόσον τηρούνται ορισμένα «συμπληρωματικά» μέτρα[99]. Τα μέτρα αυτά, όταν εξειδικεύτηκαν περιγράφονται από τις οδηγίες ως τριών κατηγοριών, ως συμβατικά μέτρα, οργανωτικά και τεχνικά. Τα συμβατικά και οργανωτικά μέτρα δεν είναι αρκετά από μόνα τους καθώς δεν μπορούν να παρακάμψουν τη νομοθεσία. Αν συμπληρωθούν όμως από τεχνικά μέτρα, εξασφαλίζεται επαρκής προστασία αφού δεν υπάρχει έτσι νόμιμος τρόπος να τα αποκτήσει η Κυβέρνηση. Συνεπώς, εταιρείες στην Αμερική μπορούν να εξασφαλίσουν το απαιτούμενο επίπεδο προστασίας σύμφωνα με το ΕΣΠΔ, αν κρυπτογραφήσουν τα δεδομένα (α) πριν την διαβίβαση, με τρόπο που δεν μπορεί να τα παραβιάσει η Κυβέρνηση ακόμα και με επίθεση εξαντλητικής αναζήτησης (brute force attack) και (β) μη αποστέλλοντας το κλειδί κρυπτογράφησης στην Αμερική, ακόμα και σε ξεχωριστή διαβίβαση ή διατηρώντας το σε άλλη Χώρα, περιορίζοντας βέβαια με αυτό τον τρόπο το είδος των δεδομένων που μπορούν να αποθηκευτούν αφού η πρόσβαση στα δεδομένα από εκεί θα είναι αδύνατη. Η ίδια αρχή μπορεί να εφαρμοστεί και με την ψευδωνυμοποίηση, μη αποστέλλοντας το κλειδί ταυτοποίησης.

[99] Βλ. Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el (τελευταία πρόσβαση 16-5-2021)

Τον Νοέμβριο του 2020 η Ευρωπαϊκή Επιτροπή ενημέρωσε τις ΤΣΡ παρουσιάζοντας δύο σετ υποδειγμάτων, οι οποίες απέκτησαν οριστική μορφή τον Ιανουάριο του 2021[100]. Τα πρώτα νέα υποδείγματα των ΤΣΡ θέτουν νέες προϋποθέσεις στους Υπεύθυνους και τους Εκτελούντες την επεξεργασία και αναπτύχθηκαν σύμφωνα με το άρθρο 29 παρ. 7 του Κανονισμού 2018/1725[101]. Αυτά θα εφαρμόζονται σε όλη την Ευρώπη και έχουν σκοπό να εξασφαλίσουν πλήρη εναρμόνιση, όταν πρόκειται για συμβάσεις μεταξύ Υπεύθυνου επεξεργασίας και Εκτελούντα την επεξεργασία. Επιπλέον, παρουσιάστηκαν και δύο νέες ΤΣΡ όσον αφορά μεταφορές δεδομένων σε τρίτες Χώρες σύμφωνα με το άρθρο 46 παρ. 2γ' του ΓΚΠΔ. Αυτές αντικαθιστούν τις ΤΣΡ που ίσχυαν βάσει της οδηγίας 95/46 και ενημερώθηκαν ώστε να είναι σύμφωνες εκτός του ΓΚΠΔ και με την απόφαση "Shrems II" και να μπορούν καλύπτουν τις πολλές περιπτώσεις ιδιότυπων επεξεργασιών που παρατηρούνται πλέον στις σύγχρονες συμβάσεις.

Με την χρήση των νέων ΤΣΡ είναι δυνατή η διαβίβαση, εφόσον κάθε οργανισμός που τις χρησιμοποιεί ή προτίθεται να τις χρησιμοποιήσει, εξετάσει το καθεστώς της χώρας που αφορά στις παρακολουθήσεις και αν κριθεί ότι δεν παρέχεται ικανοποιητικό επίπεδο προστασίας, θα πρέπει να εφαρμόσει και τα τρία συμπληρωματικά μέτρα για να επιτρέπεται η διαβίβαση και να μην πρέπει να ανασταλεί. Σε αντίθετη περίπτωση, οι επηρεαζόμενοι πολίτες μπορούν να κινηθούν νομικά εναντίον του οργανισμού για αποζημιώσεις και να υποβάλουν παράπονα ενώπιον της αρμόδιας εποπτικής Αρχής.

5.3 Σχεδιασμός ασφαλών πολιτικών

Η Πολιτική Ασφάλειας ανήκει ως έννοια στο οργανωτικό πλαίσιο της Ασφάλειας Πληροφοριών. Το οργανωτικό πλαίσιο της Ασφάλειας Πληροφοριών ενός οργανισμού περιλαμβάνει έγγραφα για πολιτικές, κανόνες, διαδικασίες και οδηγίες. Το σύνολο αυτών των εγγράφων αποτελεί το Σχέδιο Ασφάλειας.

Μια πολιτική (policy) είναι μια τυπική, σύντομη και υψηλού επιπέδου δήλωση, που εκφράζει τις γενικές πεποιθήσεις, τους σκοπούς, τους στόχους και τις αποδεκτές διαδικασίες ενός οργανισμού σε ένα συγκεκριμένο θέμα. Οι πολιτικές δεν ορίζουν ρητά τον τρόπο επίτευξης των στόχων, παρά μόνον ορίζουν τους στόχους. Για το λόγο αυτό,

[100] Βλ. https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en (τελευταία πρόσβαση 1-6-2021)

[101] Ο Κανονισμός 2018/1725 αντικατέστησε τον Κανονισμό 45/2001 και την απόφαση 1247/2002/ΕΚ (βλ. κεφ.3.3.5)

μια πολιτική συνοδεύεται από κανόνες και οδηγίες. Για έναν οργανισμό, η συμμόρφωση στην πολιτική είναι υποχρεωτική, ενώ η μη-συμμόρφωση αποτελεί πειθαρχικό παράπτωμα.

Στόχος ενός συστήματος πολιτικής ασφάλειας είναι ο περιορισμός της επικινδυνότητας σε αποδεκτό επίπεδο. Οι πολιτικές ασφάλειας προϋποθέτουν την ύπαρξη μίας δέσμης βασικών αρχών, εκφρασμένων με σαφήνεια η οποία να περιλαμβάνει τους σχεδιαστικούς στόχους των λειτουργικών συστημάτων. Κάθε αντικείμενο του συστήματος θα πρέπει να μπορεί να αναγνωρισθεί και να συνοδεύεται από μία ένδειξη του βαθμού εμπιστευτικότητας. Επιπλέον, η ισχύς των ασφαλιστικών μηχανισμών δεν θα πρέπει να βασίζεται στην άγνοια των χρηστών, σχετικά με τις τεχνικές ασφαλείας οι οποίες χρησιμοποιούνται αλλά στην αποτελεσματική τους σχεδίαση[102].

Επιπλέον, με την εφαρμογή πολιτικής ασφαλείας, θεμελιώνεται η σημασία της ασφάλειας του πληροφοριακού συστήματος για τα μέλη του οργανισμού, δημιουργείται μια κουλτούρα ασφαλείας καθώς πολλές φορές αποτελεί νομική υποχρέωση και αποτελεί παράγοντα εμπιστοσύνης μεταξύ οργανισμού και πελατών. Τα είδη των πολιτικών ασφαλείας αφορούν α) τα τεχνικά (computer oriented) συστήματα πληροφοριών, λειτουργικά συστήματα και δίκτυα υπολογιστών β) τα οργανωτικά (human oriented) ζητήματα και γ) τα ατομικά (individual security policies).

Κατά την εφαρμογή μιας πολιτικής ασφαλείας οι οδηγίες και τα μέτρα προστασίας οφείλουν να καλύπτουν το σύνολο των αγαθών και όλες τις λειτουργίες (πληρότητα) του οργανισμού. Πρέπει επίσης λαμβάνονται υπόψη οι τρέχουσες τεχνολογικές εξελίξεις και να γίνονται οι ανάλογες τροποποιήσεις ή προσθήκες ώστε να καλύπτονται τυχόν αλλαγές στο πληροφοριακό σύστημα αλλά και να είναι πάντα κατανοητές και κατάλληλες ανάλογα με τον οργανισμό που απευθύνονται.

Για να είναι επιτυχές ένα σύστημα πολιτικής ασφάλειας οφείλει να υποστηρίζει τους επιχειρηματικούς στόχους, να συμμετέχει η διοίκηση, να είναι κατάλληλο για το περιβάλλον που εφαρμόζεται, οι χρήστες να εκπαιδεύονται κατάλληλα, να υπάρχει αξιολόγηση και η πρόσβαση να είναι εύκολη και άμεση για όλους τους χρήστες του πληροφοριακού συστήματος. Τέλος, το περιεχόμενο και οι εφαρμογές πρέπει να ανανεώνονται τακτικά.

[102] Βλ. Στέφανος Γκριτζάλης, Δημήτρης Γκριτζάλης, Σωκράτης Κατσίκας, Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, 2003. σελ. 954.

5.4 Ασφαλής σχεδιασμός πληροφοριακών συστημάτων

Από μόνο του το άρθρο 25 του ΓΚΠΔ είναι κενό περιεχομένου, καθώς βασίζεται στην έννοια της προστασίας, όπως αυτή ορίζεται από άλλα άρθρα του Κανονισμού και αναφέρει ότι πρέπει να εφαρμόζονται αποτελεσματικά τα τεχνικά και οργανωτικά μέτρα[103]. Δεν ορίζεται από το άρθρο ο τρόπος που θα εκπληρωθούν αυτές οι απαιτήσεις και άρα αυτές πρέπει να εφαρμοστούν με την λήψη τεχνικών μέτρων. Τα μόνα μέτρα που επικαλείται ο Κανονισμός είναι αυτό της ψευδωνυμοποίησης[104] και υπάρχουν επίσης διάφορες αναφορές στην κρυπτογράφηση και την ανωνυμοποίηση ως προστατευτικά μέτρα (βλ. κεφ. 6 παρόντος, Τεχνολογίες ενίσχυσης της ιδιωτικότητας).

Από το άρθρο αυτό ορίζεται ότι πρέπει να λαμβάνονται υπόψη οι τελευταίες εξελίξεις, όσον αφορά την λήψη τεχνικών και οργανωτικών μέτρων. Αυτές, θα πρέπει να ερμηνευτούν ως τα κοινά πρότυπα που εφαρμόζονται στις επιχειρήσεις. Επίσης, ορίζει ότι πρέπει να λαμβάνεται υπόψη το κόστος εφαρμογής και η αποτελεσματικότητα των μέτρων με την έννοια ότι πρέπει να λαμβάνονται τα μέτρα που έχουν την καλύτερη σχέση τιμής-απόδοσης στην συγκεκριμένη εφαρμογή και όχι πάντα το αποδοτικότερο ή πιο ολοκληρωμένο. Τέλος, το άρθρο, -όταν απαιτεί να λαμβάνεται υπόψη «η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας, καθώς και οι κίνδυνοι διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία»- ενσωματώνει ουσιαστικά την απαίτηση για διενέργεια εκτίμησης αντικτύπου. Οι απαιτήσεις του άρθρου ταυτίζονται με τα οριζόμενα στο άρθρο 35 του ΓΚΠΔ, το οποίο καθορίζει τις απαιτήσεις της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

Το ΕΣΠΔ εξέδωσε στις 20 Οκτωβρίου 2020 τις κατευθυντήριες γραμμές με αριθμό 4/2019 επί του άρθρου 25 του Γενικού Κανονισμού με τις οποίες παρέχει γενικές οδηγίες σχετικά με την υποχρέωση για προστασία των δεδομένων από τον σχεδιασμό και εξ ορισμού (DPbDD) που ορίζεται στο άρθρο 25 του ΓΚΠΔ.

Από αυτές τονίζεται ότι η απαίτηση για προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού διαδραματίζει καίριο ρόλο στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων. Ως εκ τούτου, είναι σημαντικό οι υπεύθυνοι επεξεργασίας να λαμβάνουν σοβαρά υπόψη την υποχρέωση αυτή και να διασφαλίζουν την

[103] Βλ. άρθρο 25 παράγραφος 1 ΓΚΠΔ
[104] Βλ. αιτιολογική σκέψη 78 ΓΚΠΔ

προστασία των δεδομένων ήδη κατά τον σχεδιασμό δραστηριοτήτων που περιέχουν επεξεργασία προσωπικών δεδομένων.

Η απαίτηση για DPbDD δεν ισχύει μόνο για τα καινούργια συστήματα που σχεδιάζονται αλλά εφαρμόζεται και σε ήδη υπάρχοντα, εφόσον επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Οι κατευθυντήριες γραμμές περιέχουν επίσης, καθοδήγηση για την αποτελεσματική εφαρμογή των αρχών για την προστασία των προσωπικών δεδομένων του άρθρου 5 του ΓΚΠΔ, καθώς περιέχουν λίστες με τα βασικά στοιχεία της απαίτησης για προστασία των δεδομένων, ήδη από τον σχεδιασμό και εξ ορισμού.

5.4.1 Ασφαλής Σχεδιασμός Πληροφοριακών Συστημάτων (Data protection by design)

Στα πλαίσια του άρθρου 25 παρ. 1 ΓΚΠΔ, ο υπεύθυνος επεξεργασίας πρέπει να ενσωματώνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα με σκοπό να εφαρμόζονται όλες οι αρχές επεξεργασίας και να ενσωματώνονται στο σχεδιαζόμενο σύστημα τα κατάλληλα μέτρα, ώστε κατά την επεξεργασία να πληρούνται οι απαιτήσεις του νόμου αλλά και να διασφαλίζονται τα δικαιώματα των υποκειμένων. Το να είναι κατάλληλα τα μέσα σημαίνει ότι τα μέτρα είναι και αποτελεσματικά για την επίτευξη του επιδιωκόμενου σκοπού. Τα μέτρα αυτά μπορεί να είναι τεχνικά ή οργανωτικά αρκεί να διασφαλίζουν την επίτευξη του σκοπού και μπορεί να καλύπτουν από τη χρήση προηγμένων τεχνολογικών λύσεων έως τη εκπαίδευση του προσωπικού. Τέτοια μπορεί να είναι η ψευδωνυμοποίηση, όπως αναφέρεται και στον Κανονισμό ή άλλες, όπως η παροχή δυνατότητας στα υποκείμενα να έχουν πρόσβαση στα δεδομένα τους, το να υπάρχει πρόγραμμα προστασίας από κακόβουλο λογισμικό, η σωστή εφαρμογή πολιτικών λχ. καθαρού γραφείου ή η συμβατική υποχρέωση του εκτελούντα την επεξεργασία να τηρεί την αρχή της ελαχιστοποίησης.

Ο σκοπός του άρθρου 25, δεν είναι να δημιουργήσει μια συγκεκριμένη λίστα τεχνικών ή οργανωτικών μέτρων, που θα έχουν εφαρμογή σε κάθε περίπτωση. Σε κάθε συμμόρφωση οργανισμού, θα πρέπει τα μέτρα που λαμβάνονται να είναι αποτελεσματικά, ώστε να εκπληρώνεται ο σκοπός που ελήφθησαν. Σημαντικό είναι επίσης να έχουν προβλεφθεί τυχόν κίνδυνοι και να υπάρχει δυνατότητα προσαρμογής των μέτρων που έχουν ληφθεί. Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα προστασίας και ότι υπάρχουν δικλείδες ασφαλείας για

ενδεχόμενους κινδύνους που θα προκύψουν, στο μέτρο του δυνατού ανά περίπτωση, ώστε να καλύπτονται οι προϋποθέσεις του Κανονισμού.

5.4.2 Προστασία δεδομένων εξ ορισμού (Data protection by default)

Ο όρος «εξ ορισμού» κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, αναφέρεται στον όρο της προεπιλογής, όπως συναντάται στους υπολογιστές και σημαίνει ότι μια τιμή ή ρύθμιση είναι επιλεγμένη εκ των προτέρων.

Ο υπεύθυνος επεξεργασίας, θα πρέπει να σχεδιάσει το σκοπούμενο σύστημα με τρόπο ώστε να διενεργείται η κάθε επεξεργασία, μόνο όταν είναι απαραίτητη για την επίτευξη του επιδιωκόμενου σκοπού. Εάν αυτός χρησιμοποιεί λογισμικό τρίτων, θα πρέπει να είναι σε θέση να διενεργήσει αξιολόγηση κινδύνου του προϊόντος και να διασφαλίζει ότι είναι απενεργοποιημένες τυχόν άλλες λειτουργίες που δεν έχουν νομική βάση ή δεν είναι συμβατές με τους προβλεπόμενους σκοπούς επεξεργασίας. Επίσης, θα πρέπει να είναι σε θέση να διασφαλίσει ότι κατά την επεξεργασία, σύμφωνα με τις προεπιλεγμένες ρυθμίσεις, τα δεδομένα είναι μόνον όσα απαιτούνται για την επίτευξη του επιδιωκόμενου σκοπού, είτε καθορίζοντας επίπεδα πρόσβασης που απαιτούνται για κάθε μεμονωμένη επεξεργασία, είτε μειώνοντας τις κατηγορίες και τον όγκο των δεδομένων, ώστε αυτός που πραγματοποιεί την επεξεργασία να λαμβάνει μόνο τα δεδομένα που απαιτούνται για τον σκοπό αυτό. Μνεία πρέπει να γίνει και αναφορικά με την συμβατότητα του σκοπού που γίνεται η επεξεργασία σε σχέση με τον σκοπό για τον οποίο είχαν αρχικά ληφθεί τα δεδομένα. Σε περίπτωση που αυτός είναι διαφορετικός ή ενδέχεται να τροποποιηθεί, τα δεδομένα αυτά δεν μπορούν να χρησιμοποιηθούν για διαφορετικό σκοπό. Πρέπει να ελέγχεται επίσης αν έχει παρέλθει η περίοδος αποθήκευσης σε περίπτωση που δεν υπάρχει πλέον νόμιμος λόγος διατήρησής τους. Η ανωνυμοποίηση των δεδομένων είναι μια εναλλακτική της διαγραφής, υπό την προϋπόθεση ότι έχει ληφθεί υπόψη και έχει εκτιμηθεί η πιθανότητα και η σοβαρότητα των ενδεχόμενων κινδύνων, από την διατήρηση των δεδομένων πλέον των νόμιμα επιτρεπτών ορίων στην περίπτωση της επαναταυτοποίησης.

5.4.3 Απαιτήσεις του ΓΚΠΔ για ασφαλή σχεδιασμό

Ο ΓΚΠΔ θέτει τα πλαίσια και απαιτεί την εφαρμογή των αρχών προστασίας των προσωπικών δεδομένων από όλη τη νομοθεσία περί προστασίας προσωπικών δεδομένων,

καθ' όλο τον κύκλο ζωής των δεδομένων[105]. Ο κύκλος ζωής των δεδομένων περιλαμβάνει τα στάδια προστασίας των δεδομένων κατά την συλλογή, κατά την διατήρηση και ανάλυση, κατά την επεξεργασία και τέλος κατά την διαγραφή. Στην παρούσα ενότητα θα αναλυθούν οι βασικές απαιτήσεις του νόμου, ώστε να εκπληρώνονται οι αρχές αυτές και να ενσωματώνονται στο πλαίσιο του ασφαλούς σχεδιασμού.

5.4.3.1 Ασφάλεια κατά την συλλογή των δεδομένων

Κατά την διαδικασία της συλλογής των απαιτούμενων δεδομένων από το υποκείμενο των δικαιωμάτων, ο υπεύθυνος επεξεργασίας πρέπει να είναι ξεκάθαρος σχετικά με τον τρόπο με τον οποίο θα επεξεργάζεται τα προσωπικά του δεδομένα, πέραν των άλλων υποχρεώσεών του (αναφορά δικαιωμάτων κλπ.). Η αρχή της διαφάνειας, όπως αυτή ενσωματώνεται στα άρθρα 12, 13, 14 και 34 του ΓΚΠΔ απαιτεί η ενημέρωση εκ μέρους του υπεύθυνου επεξεργασίας να χαρακτηρίζεται από σαφήνεια, να είναι προσβάσιμη, κατανοητή και πολυεπίπεδη[106].

Εάν η χρήση ενός συστήματος δεν απαιτεί την καταχώρηση των χρηστών ονομαστικά ή μπορεί να γίνει μέσω τρίτων υπηρεσιών ταυτοποίησης, δεν υπάρχει λόγος να καταχωρούνται εξ αρχής τα προσωπικά στοιχεία του χρήστη και μπορεί ο προσδιορισμός τους στο σύστημα να γίνει με ψευδωνυμοποίηση. Ακολουθώντας την επιταγή του άρθρου 25 του ΓΚΠΔ, η καταχώρηση μπορεί να γίνει με την ελεύθερη επιλογή ενός ψευδώνυμου (username) με μόνο σκοπό τον προσδιορισμό του χρήστη στο σύστημα. Εξυπηρετώντας και την αρχή της ελαχιστοποίησης η καταχώρηση κάποιων στοιχείων μπορεί να γίνει με γενικευμένα χαρακτηριστικά, όπως για παράδειγμα να καταχωρείται μόνο η χρονολογία γέννησης, όταν αυτή παίζει κάποιο ρόλο στη χρήση του συστήματος αντί για την πλήρη ημερομηνία. Η χρήση των τεχνικών αυτών είναι οικονομική στον σχεδιασμό του συστήματος, εκπληρώνει τις απαιτήσεις του άρθρου 25 του ΓΚΠΔ και μειώνει τον αντίκτυπο της ενδεχόμενης απώλειάς δεδομένων.

Η λήψη συναίνεσης πρέπει να γίνεται πριν την παροχή πληροφοριών από το υποκείμενο ώστε να είναι ενημερωμένος για τους όρους της επεξεργασίας οι οποίοι πρέπει

[105] Βλ. Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework, ch. Division of Databases for Anonymized Data Processing, p.6

[106] Όπως για παράδειγμα έχει εξειδικεύσει της απαιτήσεις για διατήρηση συστήματος βιντεοεπιτήρησης, η ΑΠΔΠΧ με τις Συστάσεις με αριθμό 2/2020, https://www.dpa.gr/sites/default/files/2020-12/Sistaseis_2_2020.pdf (τελευταία πρόσβαση 12-2-2021)

να είναι διαφανείς και να καλύπτουν κάθε ενδεχόμενη χρήση των δεδομένων. Ακόμη θα πρέπει να χαρακτηρίζεται από ειδικότητα υπό την έννοια ότι θα πρέπει να αναφέρεται σε ένα μόνο συγκεκριμένο σκοπό και να μην καλύπτει εκ των προτέρων κάθε μελλοντική επεξεργασία[107]. Η συναίνεση πρέπει να δίνεται στους όρους χρήσης και την πολιτική απορρήτου ή την ενδεχόμενη χρήση cookies για διαδικτυακές εφαρμογές. Τέλος, η δήλωση συγκατάθεσης θα πρέπει να μπορεί να ανακληθεί πάντοτε[108], η ανάκληση όμως δεν μπορεί να ανακληθεί αναδρομικά αλλά ενεργεί μόνο για το μέλλον (ex nunc).

Ο υπεύθυνος επεξεργασίας περαιτέρω πρέπει να συλλέγει τα δεδομένα για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και να μην επεξεργάζεται περαιτέρω τα δεδομένα κατά τρόπο ασυμβίβαστο με τους σκοπούς για τους οποίους συλλέχθηκαν. Συνεπώς, ο σχεδιασμός της επεξεργασίας θα πρέπει να διαμορφώνεται ανάλογα με το τι απαιτείται για την επίτευξη των σκοπών. Σε περίπτωση περαιτέρω επεξεργασίας, ο υπεύθυνος επεξεργασίας πρέπει πρώτα να βεβαιωθεί ότι η επεξεργασία αυτή έχει σκοπούς συμβατούς με τους αρχικούς και να σχεδιάσει ανάλογα την επεξεργασία αυτή. Το κατά πόσον ένας νέος σκοπός είναι συμβατός ή όχι, αξιολογείται σύμφωνα με τα κριτήρια του άρθρου 6 παράγραφος 4 του ΓΚΠΔ. Ο σκοπός πρέπει να είναι προκαθορισμένος και σαφής ως προς τους λόγους για τους οποίους υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα και καθορίζει ποια δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα για την επεξεργασία. Κάθε νέος σκοπός πρέπει να είναι συμβατός με τον αρχικό σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα και ο υπεύθυνος επεξεργασίας θα πρέπει να διαφοροποιεί τον σχεδιασμό σε περίπτωση που δεν υπάρχει απόλυτη ταύτιση. Εάν χρησιμοποιούνται πολλαπλά σύνολα δεδομένων (datasets) για διαφορετικούς σκοπούς, αυτά δεν πρέπει να ενώνονται ή να αλληλοσυνδέονται ή να εκτελούνται περαιτέρω επεξεργασίες από τις προβλεπόμενες για νέους μη συμβατούς σκοπούς. Ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί τεχνικά μέτρα, συμπεριλαμβανομένης και της κρυπτογράφησης, για να περιορίσει την αλλαγή του σκοπού της επεξεργασίας των προσωπικών δεδομένων. Ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να διαθέτει τα κατάλληλα οργανωτικά μέτρα, όπως πολιτικές και συμβάσεις επεξεργασίας ή διαβίβασης με τυχόν εκτελούντες ή άλλους υπεύθυνους επεξεργασίας, τα οποία περιορίζουν την

[107] Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά Δεδομένα: Νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους, Αθήνα: Αντ. Ν. Σάκκουλας, 2007, σελ.60

[108] Βλ. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, "Νομική Διασφάλιση του απορρήτου των κινητών επικοινωνιών", ΔΙΜΕΕ 5 (Οκτ-Νοε-Δεκ 2008), σελ. 455

επαναχρησιμοποίηση δεδομένων προσωπικού χαρακτήρα, καθώς και να επανεξετάζει τακτικά κατά πόσον η επεξεργασία είναι απαραίτητη για τους σκοπούς για τους οποίους συλλέχθηκαν τα δεδομένα και να ελέγχει την συμμόρφωσή του με την απαίτηση για προστασία των δεδομένων ήδη από τον σχεδιασμό, καθώς και την αρχή του περιορισμού του σκοπού.

5.4.3.2 Ασφαλής διατήρηση και ορθότητα δεδομένων

Τα προσωπικά δεδομένα που διατηρεί κάθε οργανισμός θα πρέπει να είναι ακριβή και επικαιροποιημένα και να λαμβάνονται τα απαραίτητα μέτρα ώστε να διορθώνονται ή να διαγράφονται τα λανθασμένα άμεσα.

Η ορθότητα των προσωπικών δεδομένων είναι σημαντική γιατί μπορούν να δημιουργήσουν κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, αφού βάσει αυτών ενδέχεται να παίρνονται κρίσιμες αποφάσεις. Οι πηγές άντλησης των δεδομένων αυτών, είτε είναι με μη αυτοματοποιημένη διαδικασία είτε με αυτοματοποιημένη λήψη αποφάσεων, είτε μέσω τεχνητής νοημοσύνης, θα πρέπει να ελέγχονται διαρκώς, ώστε να διασφαλίζεται ότι τροφοδοτούν και ενημερώνουν ορθά στον οργανισμό, τα δεδομένα που επεξεργάζεται. Η χρήση νέων τεχνολογιών όπως του blockchain και της τεχνητής νοημοσύνης μπορούν να παρέχουν χρήσιμα εργαλεία και να αναβαθμίσουν το επίπεδο της ασφάλειας των οργανισμών, μειώνοντας την ανακρίβεια των δεδομένων, αυξάνοντας την ταχύτητα ενημέρωσης και συνεπώς της αξιοπιστία και την εμπιστοσύνη στο οργανισμό.

Τα προσωπικά δεδομένα πρέπει να διατηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων για χρονικό διάστημα που δεν υπερβαίνει το αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα. Τα μέτρα και οι εγγυήσεις που εφαρμόζουν την αρχή του περιορισμού της αποθήκευσης συμπληρώνουν τα δικαιώματα της διαγραφής και της εναντίωσης. Οι οργανισμοί θα πρέπει να είναι συνεπείς στην διαγραφή δεδομένων και να προχωρούν σε τεχνικές ανωνυμοποίησης. Πρέπει να υπάρχει επαρκής αιτιολογία για την διατήρηση των στοιχείων, να υπάρχουν και να ενημερώνονται οι πολιτικές διατήρησης των δεδομένων και να περιορίζονται γενικά οι προσωρινές λύσεις όσον αφορά τους τομείς αυτούς, όταν δεν είναι η άμεση αλλαγή του σχεδιασμού.

Ενδιαφέρουσα λύση που ενισχύει την ανωνυμία, αποτελεί και η εφαρμογή της τεχνικής του διαχωρισμού[109] των βάσεων δεδομένων. Με αυτή τη λύση υπάρχουν δύο βάσεις δεδομένων, μια η οποία θα κρατάει τα δεδομένα που είναι προς επεξεργασία καταχωρώντας μόνο ως αναγνωριστικό ένα μοναδικό αριθμό που αντιστοιχεί στον χρήστη και μια δεύτερη βάση δεδομένων η οποία θα κρατάει μόνο τα προσωπικά δεδομένα του κάθε χρήστη και βάσει της οποία μπορεί να ταυτοποιηθεί ο κάθε χρήστης με βάση τον μοναδικό του αριθμό. Αυτή είναι και η αρχή, επί της ουσίας, που εφαρμόζεται και σε υπηρεσίες ταυτοποίησης χρηστών, όπου ένας οργανισμός διαχειρίζεται τα προσωπικά δεδομένα και δίνει την δυνατότητα σε τρίτους να πιστοποιούν χρήστες μέσω αυτού[110], χωρίς οι τρίτοι να λαμβάνουν ποτέ προσωπικά στοιχεία των χρηστών.

Γίνεται συνεπώς αντιληπτό ότι πραγματική ανωνυμία δεν μπορεί να επιτευχθεί με τη χρήση μίας μόνο τεχνικής, αλλά με συνδυασμό διαφόρων τεχνικών με σκοπό την βελτίωση της ασφάλειας, τεχνικές οι οποίες θα πρέπει πρώτα να εφαρμόζονται στο πλαίσιο της ασφάλειας εκ του σχεδιασμού (βλ. κεφ. 6.4 «Η απόκρυψη της ταυτότητας»).

5.4.3.3 Τήρηση αρχών κατά την επεξεργασία

Ο υπεύθυνος επεξεργασίας πρέπει να καθορίζει μια έγκυρη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τα μέτρα και οι διασφαλίσεις θα πρέπει να εξασφαλίζουν ότι ολόκληρος ο κύκλος ζωής της επεξεργασίας είναι σύμφωνος με την νομική αυτή βάση. Κάθε επεξεργασία θα πρέπει να είναι αναγκαία και να στηρίζεται στην ορθή νομική βάση και να συνδέεται με σαφήνεια με τον επιδιωκόμενο σκοπό επεξεργασίας. Η νομική βάση θα πρέπει να καθορίζεται πριν από την επεξεργασία και εάν σταματήσει να ισχύει, θα πρέπει να παύει και η επεξεργασία.

Η αρχή της αντικειμενικότητας απαιτεί να μην γίνεται επεξεργασία των δεδομένων προσωπικού χαρακτήρα κατά τρόπο επιζήμιο ή παραπλανητικό για το υποκείμενο των δικαιωμάτων, να γίνονται σεβαστά τα θεμελιώδη δικαιώματά και η αξιοπρέπεια του και να του παρέχεται η δυνατότητα να ασκεί τα δικαιώματα που του παρέχονται από τον ΓΚΠΔ. Ο υπεύθυνος επεξεργασίας θα πρέπει να αναλαμβάνει την ευθύνη του από την επεξεργασία και μην μεταφέρει τον κίνδυνο της επιχείρησής του στα υποκείμενα των δεδομένων.

[109] Βλ. Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework, ch. Division of Databases for Anonymized Data Processing, p.220
[110] Βλ. Υπηρεσία «oauth», https://oauth.net/, (τελευταία πρόσβαση 3-2-2021)

Η αρχή της ελαχιστοποίησης[111] των δεδομένων επιβάλλει στον υπεύθυνο επεξεργασίας να επεξεργάζεται μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι κατάλληλα, συναφή και περιορισμένα στο αναγκαίο για τον σκοπό επεξεργασίας. Αυτό επιτυγχάνεται, όταν διαμορφώνεται με τέτοιο τρόπο η επεξεργασία, ώστε να έχει πρόσβαση μόνο στα απολύτως απαραίτητα δεδομένα ο ελάχιστος δυνατός αριθμός ατόκων για τον σκοπό της εκτέλεσης των καθηκόντων τους. Χρήσιμα εργαλεία για την επίτευξη της αρχής είναι η χρήση της ψευδωνυμοποίησης, της ανωνυμοποίησης και γενικευμένων δεδομένων, όπως και η εφαρμογή χρήσης απομονωμένων βάσεων δεδομένων.

Κατά την επεξεργασία είναι σημαντική επίσης και η τήρηση των αρχών της ακεραιότητας και της εμπιστευτικότητας με σκοπό την προστασία από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή ζημία, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων. Τα μέτρα που λαμβάνονται θα πρέπει να υπηρετούν τις παραπάνω αρχές και να αποδεικνύεται ότι είναι κατάλληλα και αποτελεσματικά.

5.4.3.4 Ασφάλεια κατά την διαγραφή

Το δικαίωμα στη λήθη αποτελεί ένα κανονιστικό εργαλείο, για να επιτρέπει στα υποκείμενα των δικαιωμάτων να διατηρούν τον έλεγχο των δεδομένων τους στον ψηφιακό κόσμο[112]. Το δικαίωμα στη φορητότητα αποτελεί επίσης ένα ακόμα ενισχυτικό στοιχείο της προστασίας των πληροφοριών του υποκειμένου, ώστε να μπορεί το υποκείμενο να διαγράφει και έπειτα να διαβιβάζει τα δεδομένα του ελεύθερα[113]. Τα δύο αυτά δικαιώματα -όπως αναφέρεται και στην αιτιολογική σκέψη 62 και άρθρο 20 του ΓΚΠΔ- είναι συνδεδεμένα και σε περίπτωση άσκησης του ενός δεν περιορίζεται η δυνατότητα άσκηση του άλλου. Για να θεωρηθεί ότι εκπληρώνονται οι απαιτήσεις της ασφάλειας εκ του σχεδιασμού, ο κάθε οργανισμός πρέπει να έχει ενημερωμένες πολιτικές όσον αφορά την διατήρηση και την διαγραφή[114] των δεδομένων, είτε λόγω αιτήματος διαγραφής είτε λόγω

[111] Για την αρχή της ελαχιστοποίησης που διέπει τον ΓΚΠΔ βλ. αναλυτικά σε Λ.Μήτρου, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, 2017, σελ. 63 επ.

[112] Βλ. Λ.Μήτρου, Ο Γενικός Κανονισμός Προσωπικών Δεδομένων, 2017, σελ. 131

[113] Βλ. Λ.Μήτρου, ο.π. σελ.135

[114] Για το δικαίωμα στη λήθη βλ. Λ. Μήτρου, Η δημοσιότητα της κύρωσης ή η κύρωση της δημοσιότητας, 2012, σελ. 156-163, Παναγοπούλου – Κουτνατζή Φ., Το δικαίωμα στη λήθη στην εποχή της αβάσταχτης μνήμης: Σκέψεις αναφορικά με την Πρόταση Κανονισμού Προστασίας Δεδομένων, ΕφημΔΔ 2012, 264 επ. Για τη διαφορά του ως άνω δικαιώματος με το νέο δικαίωμα στη ψηφιακή λήθη βλ.Ι. Ιγγλεζάκη, Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, 2014, σελ. 34 και 82.

άσκησης του δικαιώματος στη φορητότητα. Ο σκοπός είναι τα δεδομένα να διατηρούνται για όσο χρονικό διάστημα απαιτείται για να εκπληρωθεί ο σκοπός τους ή μέχρι να εκλείψουν οι απαιτήσεις του νόμου για τη διατήρησή τους.

Εφόσον πληρούνται οι όροι διαγραφής δεδομένων, ειδική μνεία πρέπει να λαμβάνεται για την διαγραφή των δεδομένων και από τα αντίγραφα ασφαλείας αυτών. Τα αντίγραφα ασφαλείας πρέπει να βρίσκονται ιδανικά σε διαφορετική τοποθεσία αποθήκευσης και να ενημερώνονται τακτικά, ώστε σε περίπτωση απώλειας δεδομένων, να μειώνεται ο αντίκτυπος της επελθούσης ζημίας. Η προσθήκη ημερομηνίας λήξης στα δεδομένα και η ενημέρωσή της με αυτόματους τρόπους, αποτελεί μια πολύ καλή πρακτική για την έγκαιρη διαγραφή, όταν απαιτείται.

Η κάθε διαγραφή επίσης, θα πρέπει να καταγράφεται πότε συνέβη και τι περιελάβανε μέσω ενός πρωτοκόλλου διαγραφής. Η καταγραφή αυτή εξασφαλίζει ότι τα δεδομένα χειρίζονται από τον οργανισμό με τρόπο σύμφωνο με τις εσωτερικές οδηγίες και πολιτικές του, αλλά και ότι τηρείται ο περιορισμός στην πρόσβαση στα εξουσιοδοτημένα άτομα προς αυτό το σκοπό.

5.4.4 Προβλήματα στην ενσωμάτωση και χρήση του ασφαλούς σχεδιασμού

Η ενσωμάτωση τεχνολογιών ή διαδικασιών με σκοπό την αύξηση της ασφάλειας εκ του σχεδιασμού απαιτεί επιπλέον οικονομικούς πόρους για τους οργανισμούς. Πολλά δε από τα προσφερόμενα εργαλεία, χρησιμοποιούν νέες ακριβές τεχνολογίες. Η ομομορφική κρυπτογράφηση (βλ. κεφ. 6.4.4) για παράδειγμα απαιτεί μεγάλους υπολογιστικούς πόρους για να εφαρμοστεί και πρακτικά δεν είναι εφαρμόσιμη στην πλειονότητα των οργανισμών, όπου το κόστος ενσωμάτωσης της τεχνολογίας και συντήρησης του εξοπλισμού είναι δυσανάλογα μεγάλο σε σχέση με την ευθύνη που έχουν για προστασία των δεδομένων που κατέχουν. Επίσης, η πρόσβαση σε προσωπικά δεδομένα για διαφημιστικούς σκοπούς, αποτελεί ένα τεράστιο εμπορικό πλεονέκτημα που αυξάνει πάντα τις πωλήσεις ιδίως των διαδικτυακών προϊόντων και αποφέρει μεγάλο οικονομικό όφελος στις επιχειρήσεις που τα κατέχουν. Για αυτό πολλές επιχειρήσεις είναι απρόθυμες να ενσωματώσουν ασφαλέστερα συστήματα ή τεχνικές ανωνυμοποίησης, που ενδέχεται να μειώσουν τα κέρδη αυτά. Στις εταιρίες που προσφέρουν υπηρεσίες cloud επίσης, υπάρχουν ορισμένα προβλήματα στην ενσωμάτωση τέτοιων τεχνικών, καθώς απαιτείται τα δεδομένα των χρηστών να είναι άμεσα προσβάσιμα σε αναγνώσιμη μορφή

και μη κρυπτογραφημένα, ώστε να μπορούν να παρασχεθούν ορισμένες υπηρεσίες όπως λχ. αναζήτησης ή αναγνώρισης κειμένου. Ένα επιπλέον εμπόδιο στην ενσωμάτωση τεχνολογιών ασφάλειας σε πληροφοριακά συστήματα είναι και το θέμα της διαλειτουργικότητας. Όσο περισσότερες τεχνικές ασφαλείας ενσωματώνονται σε ένα σύστημα, τόσο περισσότερο μειώνεται η διαλειτουργικότητά του με άλλα ακόμα και η συμβατότητά του με προηγούμενες εκδόσεις του ίδιου του συστήματος καθιστώντας έτσι δυσκολότερη τη λειτουργία και τη συντήρησή του.

Το διαδίκτυο των πραγμάτων (IoT) και τα μεγάλα δεδομένα (big data) θέτουν και αυτά σοβαρές προκλήσεις στην εφαρμογή των εργαλείων ανωνυμοποίησης, λόγω της δυνατότητας επαναταυτοποίησης μέσω νέων τεχνικών (βλ. κεφ. 4.6.5) αλλά κυρίως λόγω του ότι οι διαθέσιμες πληροφορίες για κάθε υποκείμενο πληθαίνουν από διάφορες πηγές, καθιστώντας έτσι ακόμα πιο δύσκολη την απόκρυψη της ταυτότητας και την αξιοπιστία των τεχνικών ανωνυμοποίησης. Συνεπώς, πρέπει να λαμβάνεται υπόψη πριν την εφαρμογή μιας τεχνικής ανωνυμοποίησης, το κόστος που θα έχει για την ενσωμάτωση σε κάθε οργανισμό αλλά το επίπεδο ευκολίας με το οποίο μπορεί να γίνει επαναταυτοποίηση των ανωνυμοποιημένων δεδομένων, έτσι ώστε να αξιολογείται συνολικά η αποδοτικότητα του μέτρου.

Προβλήματα μπορεί να προκύψουν επίσης και στην εφαρμογή τεχνικών μέτρων που προάγουν την αυτονομία, όπως η διαγραφή δεδομένων και η φορητότητα, όπως αναφέρθηκε παραπάνω (κεφ. 5.4.3.4). Τα τεχνικά μέτρα προς αυτό το σκοπό είναι συνήθως δύσκολο να ενσωματωθούν γιατί οι οργανισμοί που τα εφαρμόζουν συνήθως κατευθύνονται στην τήρηση ενός απλού αντιγράφου (ακόμα και σε κάρτες μνήμης), με ελάχιστη αξιοπιστία ως προς το ενδεχόμενο καταστροφής, απώλειας ή κλοπής του. Η εφαρμογή επίσης των πολιτικών ασφαλείας (κεφ. 5.3) δεν φαίνεται να αποδίδει στην πράξη, αφού τα περιστατικά απώλειας εμπιστευτικότητας είναι πολλαπλά, ακόμα και από οργανισμούς με μεγάλο κύκλο συναλλαγών (κεφ. 6.4.5).

Πρέπει συνεπώς να αναζητηθεί ο τρόπος που μπορεί η νομοθεσία να αντιπαρέλθει σε αυτές τις προκλήσεις. Βέβαια όλα τα προβλήματα που εκτέθηκαν δεν μπορούν να λυθούν με τεχνικής φύσης εργαλεία, καθώς οι πηγές των προβλημάτων μπορούν να είναι και άλλες, όπως η έλλειψη ευαισθητοποίησης, οργανισμών και υποκειμένων ως προς την ανάγκη εφαρμογής των μέτρων αλλά και η προβληματική ενσωμάτωση διαφόρων τεχνικών από τους υπεύθυνους επεξεργασίας ή προγραμματιστές των εφαρμογών που

χρησιμοποιούν. Τα προβλήματα αυτά μπορούν να διορθωθούν με την ενσωμάτωση νομοθετικών εργαλείων, ώστε συνδυασμένα με τα τεχνικά εργαλεία να προσφέρουν μεγαλύτερη προστασία. Αυτό που απαιτείται περισσότερο είναι οι νομοθετικοί κανόνες να διαμορφώνονται με βάση τις τεχνικές προκλήσεις αλλά και να ακολουθούν τις τεχνολογικές εξελίξεις και οι σχεδιαστές των εφαρμογών προστασίας της ιδιωτικότητας να είναι εκπαιδευμένοι και σε νομικά θέματα, ώστε να αναπροσαρμόζουν τον σχεδιασμό των εφαρμογών με τρόπο που να καλύπτονται οι απαιτήσεις του νόμου. Η νομοθεσία πρέπει να απαιτεί την εφαρμογή συγκεκριμένων μέτρων ασφάλειας (λχ. υποχρεωτικότητα εφαρμογής της τεχνικής της γενίκευσης δεδομένων, ή την υποχρεωτική εφαρμογή τουλάχιστον δύο τεχνικών ανωνυμοποίησης για κάποια συγκεκριμένη κατηγορία δεδομένων) και η τεχνολογία να γίνει το μέσο εφαρμογής των απαιτήσεων του Νόμου. Η εφαρμογή της ασφάλειας -εκ του σχεδιασμού και εξ ορισμού- ενισχύει την συμπληρωματική σχέση του Νόμου και της τεχνολογίας και μπορεί να προσφέρει πολλές λύσης ενίσχυσης της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων.

6 ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΕΝΙΣΧΥΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Στο συγκεκριμένο κεφάλαιο θα αναλυθούν οι κρίσιμες τεχνολογίες και τεχνικές με τις οποίες μπορεί να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας μέσω της χρήσης προηγμένων εργαλείων και τεχνικών. Επιπλέον, θα αναλυθούν στοιχεία της κρυπτογραφίας με την οποία μπορεί να γίνει ασφαλής μια διαβίβαση δεδομένων. Επίσης, θα γίνει μια αντιπαράθεση των διαφόρων τεχνικών της ανωνυμοποίησης και της ψευδωνυμοποίησης, όπως και των τεχνολογιών που χρησιμοποιούνται σήμερα για να επιτευχθεί η ανωνυμία των υποκειμένων των δεδομένων, όταν στοιχεία τους καταχωρούνται σε σύνολα δεδομένων.

6.1 Ενίσχυση της ασφάλειας

Στους σκοπούς της ενίσχυσης της ασφάλειας συμπεριλαμβάνεται η αποφυγή αδυναμιών, ο εντοπισμός απειλών, η πρόληψη ατυχημάτων και η μείωση του κινδύνου. Οι τρωτότητες του συστήματος που πρέπει να προστατευτεί καθορίζουν το είδος των απειλών[115] που θα πρέπει να αντιμετωπιστούν από τους σχεδιαστές του μηχανισμού ασφαλείας[116]. Η αναγνώριση των απειλών αυτών, η συσχέτισή τους με ευπάθειες συγκεκριμένων αγαθών και η αποτίμηση των πιθανών συνεπειών από την εκμετάλλευσή τους (επιθέσεις) ονομάζεται ανάλυση επικινδυνότητας (risk analysis). Η μελέτη για τη λήψη των μέτρων προστασίας στη βάση των αποτελεσμάτων ανάλυσης επικινδυνότητας γίνεται στο πλαίσιο της επόμενης φάσης της αντιμετώπισης επικινδυνότητας (risk treatment), γι' αυτό ολόκληρη η διαδικασία ονομάζεται διαχείριση επικινδυνότητας (risk management). Ο σκοπός της διαχείρισης επικινδυνότητας είναι να επιτευχθεί το επιδιωκόμενο επίπεδο ασφαλείας με ορθολογική λήψη αποφάσεων που μετρούν το κόστος των μέσων και του χρόνου που θα απαιτηθεί. Για την πιστοποίηση της καταλληλότητας των μέτρων χρησιμοποιείται η σειρά προτύπων ISO/IEC 27000, η οποία είναι ένας οδηγός βέλτιστων πρακτικών για τη διαχείριση της ασφάλειας πληροφοριών και τη διαχείριση της σχετικής επικινδυνότητας που αντιμετωπίζει ένας οργανισμός. Το κεντρικό πρότυπο είναι το ISO/IEC 27001 με το οποίο μπορεί ένας οργανισμός να εναρμονιστεί και να λάβει

[115] Stapleton, pp. 42-44.
[116] Stapleton, pp. 51-52.

πιστοποίηση από τρίτο ανεξάρτητο φορέα. Ο φορέας πιστοποίησης με τη σειρά του μπορεί να λάβει διαπίστευση, σύμφωνα με το πρότυπο ISO/IEC 27006. Το πρότυπο ISO 27000 ορίζει την ασφάλεια των πληροφοριών ως «διατήρηση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών».

Τήρηση της αρχής της εμπιστευτικότητας σημαίνει ότι υπάρχουν επαρκείς εξασφαλίσεις στο σχεδιαζόμενο σύστημα ότι οι πληροφορίες που διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται, δεν αποκαλύπτονται σε μη εξουσιοδοτημένα μέρη. Σαν έννοια δεν πρέπει να συγχέεται με την ιδιωτικότητα, καθώς αυτή αποτελεί πιο ευρεία έννοια[117]. Ακεραιότητα σημαίνει ότι οι πληροφορίες που διαβιβάζονται, αποθηκεύονται ή επεξεργάζονται δεν παράγονται, τροποποιούνται ή διαγράφονται από μη εξουσιοδοτημένα μέρη. Διαθεσιμότητα σημαίνει ότι οι πόροι του πληροφοριακού συστήματος παραμένουν προσβάσιμοι στους εξουσιοδοτημένους χρήστες, όποτε τους χρειάζονται. Εκτός των βασικών αυτών ιδιοτήτων ασφάλειας, μέρη της ασφάλειας των πληροφοριακών συστημάτων, όπως ειπώθηκε ήδη, είναι και η διασφάλιση των αρχών της αυθεντικότητας, της λογοδοσίας, της ύπαρξης δυνατότητας ελέγχου, της αδυναμίας αποποίησης και της αξιοπιστίας[118].

Οι παραπάνω εγγυήσεις με σκοπό την ασφάλεια των πληροφοριακών συστημάτων από τεχνικής άποψης επιτυγχάνονται μέσω της εφαρμογής τεχνολογιών ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies ή PETs)[119], οι οποίες αποτέλεσαν και την βάση της έννοιας της εκ του σχεδιασμού ιδιωτικότητας (privacy by design)[120]. Αυτές αναπτύχθηκαν προκειμένου να ενισχύσουν την προστασία της ιδιωτικότητας στα σύγχρονα πληροφοριακά και επικοινωνιακά συστήματα και σύμφωνα με την Λ. Μήτρου προσδιορίζονται ως «ένα ολοκληρωμένο σύστημα μέτρων ΤΠΕ[121] που προστατεύουν την ιδιωτικότητα, εξαλείφοντας ή περιορίζοντας τη μη αναγκαία αποκάλυψη, συλλογή, τήρηση, διαμοιρασμό των προσωπικών δεδομένων, συχνά με την παροχή εργαλείων για

[117] cf. Brenner et al., pp. 3-5; Camp, p. 69; Stapleton, p. 211.

[118] ISO/IEC 27000: 2016, Art. 2.33; σύμφωνα με τον Avižienis et al., p. 23 «accountability, authenticity, and non-repudiability are secondary attributes of security»; cf. Camp, pp. 73-77

[119] Λ. Μήτρου, Privacy by Design Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔΙΤΕ (π. ΔΙΜΕΕ), τεύχος 1/2013, Κεφάλαιο «Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας».

[120] Βλ. και International Conference of Data Protection and Privacy Commissioners, Privacy by Design Resolution (Jerusalem 2010)

[121] ο.π. και εκεί παραπομπή M. van Lieshout, L. Kool, B. van Schoonhoven and M. de Jong, Privacy by Design: an alternative to existing practice in safeguarding privacy Info Vol. 13 No 6 (2011), pp. 55-68

την ενίσχυση του ελέγχου του ατόμου πάνω στα προσωπικά του στοιχεία, και χωρίς να απομειώνεται η λειτουργικότητα των πληροφοριακών συστημάτων».

Παρακάτω, θα αναλυθούν εφαρμοζόμενες τεχνολογίες και τεχνικές στον τομέα της ιδιωτικότητας, που μπορούν να προσφέρουν λύσεις στην προστασία των προσωπικών δεδομένων.

6.2 Κρυπτογραφία

Σημαντικό εργαλείο ενίσχυσης της ασφάλειας είναι η κρυπτογραφία. Αυτή, αποτελεί την διαδικασία μετατροπής ενός μηνύματος (encryption) χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης και έπειτα την επαναφορά του με έναν αλγόριθμο αποκρυπτογράφησης. Με αυτόν τον τρόπο, μπορεί να διασφαλιστεί τόσο η εμπιστευτικότητα (οι πληροφορίες που μετατρέπονται από έναν αλγόριθμο γίνονται δυσανάγνωστες και μπορούν να διαβαστούν μόνο με την επαναφορά τους στην αρχική τους μορφή), όσο και η ακεραιότητα (με την αξιοποίηση της κρυπτογραφίας για την παραγωγή ψηφιακών υπογραφών) των πληροφοριών.

Στον ΓΚΠΔ δεν περιλαμβάνεται ένας ακριβής ορισμός της χρήσης της κρυπτογραφίας για την προστασία της εμπιστευτικότητας. Ωστόσο, ο ορισμός αυτός θα μπορούσε να διατυπωθεί ως η εφαρμογή μιας διαδικασίας μετατροπής με τη χρήση κλειδιού κρυπτογράφησης, ενός συνόλου προσωπικών δεδομένων σε μία ακατανόητη μορφή, ώστε να μην μπορούν να αναγνωσθούν από κανέναν εκτός από τον κάτοχο του κλειδιού αποκρυπτογράφησης.

Η κρυπτογραφία έχει τέσσερις βασικούς αντικειμενικούς σκοπούς[122]:

- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα: Η πληροφορία δεν μπορεί να αλλοιώνεται χωρίς να ακολουθεί ανίχνευση της αλλοίωσης.
- Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να απαρνηθεί την αποστολή ή την παραλαβή της.
- Αυθεντικότητα: Ο παραλήπτης μπορεί να εξακριβώνει την ταυτότητα του αποστολέα.

[122] https://el.wikipedia.org/wiki/Κρυπτογραφία (τελευταία πρόσβαση 14-1-2021)

6.2.1 Εισαγωγή στην κρυπτογραφία

Βασικά συστατικά ενός κρυπτοσυστήματος είναι το απλό κείμενο (plaintext) «M», δηλαδή το κείμενο στην αρχική του μορφή, το κρυπτοκείμενο (ciphertext) «C», το οποίο είναι το κείμενο στην κρυπτογραφημένη του μορφή, ο αλγόριθμος κρυπτογράφησης (encryption algorithm) «e(*)», ο οποίος είναι η μέθοδος που χρησιμοποιείται για να κρυπτογραφηθεί το μήνυμα και ο αλγόριθμος αποκρυπτογράφησης (decryption algorithm) «d(*)». Οπότε για την κρυπτογράφηση ενός κειμένου χρησιμοποιείται ο τύπος «C = e(M)» και για την αποκρυπτογράφηση ο τύπος «M = d(C)»[123]. Βασική απαίτηση, για να μπορεί η μέθοδος της κρυπτογράφησης να παρέχει ασφάλεια στην επικοινωνία, είναι να υπάρχει και ένα κλειδί κρυπτογράφησης «K».

6.2.2 Συμμετρική και ασύμμετρη κρυπτογραφία

Η κλασσική μέθοδος κρυπτογραφίας είναι η λεγόμενη συμμετρική ή κρυπτογραφία συμμετρικού κλειδιού (symmetric-key, secret-key, single-key). Σε αυτή υπάρχει ένα κλειδί και χρησιμοποιείται το ίδιο στην κρυπτογράφηση και στην αποκρυπτογράφηση. Ο τύπος που χρησιμοποιείται σε αυτή τη περίπτωση είναι για την κρυπτογράφηση ο «C = e(M,K)» και για την αποκρυπτογράφηση ο «M = d(C,K)». Μειονέκτημα αποτελεί το γεγονός ότι αν ο αποστολέας και ο παραλήπτης είναι σε διαφορετικές τοποθεσίες, θα πρέπει να βρουν ένα ασφαλές τρόπο να ανταλλάξουν μεταξύ τους το κλειδί.

Μια μέθοδος κρυπτογράφησης, που χρησιμοποιήθηκε ευρέως αλλά πλέον έχει αποσυρθεί, είναι η Data Encryption Standard (DES)[124], η οποία χρησιμοποιεί blocks δεδομένων αρχικού κειμένου των 64 bit και κλειδί μεγέθους 64 bit, τα 8 εκ των οποίων χρησιμοποιούνται για έλεγχο λάθους. Σε αυτή τη μέθοδο, η κρυπτογράφηση και η αποκρυπτογράφηση είναι αναστρέψιμες διαδικασίες, δηλαδή το ίδιο κλειδί και τα ίδια βήματα χρησιμοποιούνται κατά την αποκρυπτογράφηση, για να αναστρέψουν την κρυπτογράφηση[125]. Το μικρό όμως μέγεθος του κλειδιού DES, ακόμη και μετά τη βελτιωμένη έκδοση του 3DES, η οποία έκανε την διαδικασία 3 φορές και χρησιμοποιώντας 3 κλειδιά, καθιστά το DES μη ανθεκτικό για τους σημερινούς

[123] Αφού C = e(M) τότε για να βρεθεί το αρχικό κείμενο M = d(e(M)) = d(C)
[124] Βλ. https://el.wikipedia.org/wiki/Data_Encryption_Standard
[125] Brooks, pp. 83-85; Schmeh, p. 86; Stallings, p. 92.

υπολογιστές[126]. Σήμερα χρησιμοποιείται η μέθοδος Advanced Encryption Standard (AES), που κρυπτογραφεί blocks των 128, 192 ή 256 bit[127].

Στην προσπάθεια να δοθεί λύση στο πρόβλημα της ανταλλαγής συμμετρικών κλειδιών, διαπιστώθηκε ότι ένα κρυπτοσύστημα δεν πρέπει κατ' ανάγκη να είναι συμμετρικό. Η διαπίστωση αυτή αποτέλεσε τη σημαντικότερη εξέλιξη της σύγχρονης κρυπτογραφίας και οδήγησε στην ανάπτυξη της ασύμμετρης κρυπτογραφίας. Ένα κρυπτοσύστημα στο οποίο κάθε μέρος διαθέτει ένα τουλάχιστον ζεύγος κλειδιών (δημόσιο και ιδιωτικό) λέγεται ότι είναι ένα ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημόσιου κλειδιού (asymmetric ή public key cryptography). Στην ασύμμετρη κρυπτογραφία χρησιμοποιείται διαφορετικό κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση, δηλαδή το δημόσιο (public) κλειδί που μπορεί να το δει οποιοσδήποτε και το ιδιωτικό (private) κλειδί το οποίο είναι απόρρητο, αλλά του ιδίου ζεύγους. Σύμφωνα με τον Ι.Μαυρίδη[128], οι ασύμμετροι αλγόριθμοι λειτουργούν ικανοποιώντας δυο (2) βασικές απαιτήσεις, πρώτον ότι είναι υπολογιστικά ανέφικτο να υπολογιστεί το ένα κλειδί γνωρίζοντας το άλλο κλειδί του ίδιου κατόχου και δεύτερον ότι κάθε αρχικό κείμενο που κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται μόνο με το άλλο κλειδί του ίδιου ζεύγους.

Με αυτό τον τρόπο, κάθε χρήστης έχει τουλάχιστον ένα ζεύγος κλειδιών, με ένα δημόσιο κλειδί[129] και ένα ιδιωτικό. Κάθε δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, οπότε πρέπει να διαδοθεί. Το μόνο που απαιτείται είναι να πιστοποιείται η σύνδεση του δημόσιου κλειδιού με την πραγματική ταυτότητα του χρήστη-ιδιοκτήτη του. Το ιδιωτικό κλειδί αντίθετα δεν μεταδίδεται ποτέ, το χρησιμοποιεί ο κάθε χρήστης τοπικά για να αποκρυπτογραφήσει το μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί του. Για παράδειγμα, ο χρήστης Α θέλει να στείλει ένα κρυφό μήνυμα στον Β. Ο Α χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα και το στέλνει στον Β. Ο Β έπειτα χρησιμοποιεί το δικό του ιδιωτικό κλειδί, για να αποκρυπτογραφήσει

[126] Cozzens/Miller, p. 13; Garrett, p. 100; Ferguson/Schneier, pp. 51-54; Ferguson/Schneier/Kohno, p. 51; Schmeh, pp. 89-91.

[127] Brooks, pp. 85-87; Ferguson/Schneier, p. 55; Ferguson/Schneier/Kohno, pp. 54-56; Mollin, p. 152; Pfleeger/Pfleeger, pp. 73-75; Schmeh, pp. 127-129; Wu/Irwin, p. 920.

[128] Μαρίδης Ι., Ασφάλεια Πληροφοριών στο Διαδίκτυο, σελ. 108

[129] Το δημόσιο κλειδί είναι ένας τυχαίος αριθμός ο οποίος συνήθως αποτελείται από πολλά ψηφία και αποτελεί ουσιαστικά τη δημόσια διεύθυνση του κάθε χρήστη. Μπορεί να γνωστοποιηθεί σε τρίτους, και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων ενώ το ιδιωτικό για την αποκρυπτογράφηση.

το μήνυμα. Με αυτόν τον τρόπο και το μήνυμα στάλθηκε κρυπτογραφημένο για προστασία της εμπιστευτικότητας και το πραγματικό κλειδί που θα κάνει την αποκρυπτογράφηση δεν στάλθηκε ποτέ, ούτε καν το γνωρίζει ο Α. Τώρα αν ο Α θέλει και να υπογράψει αυτό το μήνυμα, τότε για την παραγωγή της υπογραφής του το κρυπτογραφεί με το ιδιωτικό του κλειδί και το αποτέλεσμα το στέλνει μαζί με το μήνυμα. Για να επαληθεύσει ο Β την ψηφιακή υπογραφή του Α, θα αποκρυπτογραφήσει το μήνυμα με το δημόσιο κλειδί του Α (προστασία ακεραιότητας, αυθεντικότητας και μη-απάρνησης).

Η ασύμμετρη κρυπτογραφία πλεονεκτεί σε ό,τι αφορά την ανταλλαγή των κλειδιών, αλλά μειονεκτεί στο ό,τι απαιτεί μεγαλύτερη υπολογιστική ισχύ από την συμμετρική, η οποία είναι ευκολότερα εφαρμόσιμη σε περιπτώσεις μικρών συσκευών, όπως για παράδειγμα οι IoT συσκευές.

6.3 Μέτρα ενίσχυσης της ακεραιότητας, της αυθεντικότητας και της μη-απάρνησης

Η ακεραιότητα, η αυθεντικότητα και η μη-απάρνηση είναι έννοιες που αλληλοσυνδέονται και υποστηρίζονται από μηχανισμούς όπως οι ψηφιακές υπογραφές.

6.3.1 Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές είναι το προσφορότερο μέσο για να εξασφαλιστεί το επιθυμητό επίπεδο ελέγχου ακεραιότητας και αυθεντικότητας. Για αυτό το σκοπό, θα πρέπει να μπορεί ο παραλήπτης να επαληθεύει την πηγή των δεδομένων και το περιεχόμενό τους κατά την παραλαβή του μηνύματος από τον ορθό παραλήπτη και να μπορεί να εγγυηθεί ότι ο χρήστης δεν θα μπορεί να αρνηθεί ότι έλαβε το μήνυμα. Η σύγχρονη κρυπτογραφία, προσφέρει τις δυνατότητες αυτές, ιδίως μέσω της ασύμμετρης κρυπτογραφίας (βλ. κεφ. 6.2.2. ασύμμετρη κρυπτογραφία)[130].

6.3.2 Συναρτήσεις κατακερματισμού

Για την δημιουργία ψηφιακών υπογραφών, απαιτείται να κωδικοποιηθεί η σύνοψη (hash[131]) του μηνύματος χρησιμοποιώντας μια συνάρτηση κατακερματισμού ή ένα

[130] Βλ. https://el.wikipedia.org/wiki/RSA (τελευταία πρόσβαση 12-2-2021)

[131] Το hash είναι μια σειρά από αριθμούς και γράμματα που παράγονται από μία συνάρτηση. Μια συνάρτηση hash είναι μια μαθηματική συνάρτηση που παίρνει έναν μεταβλητό και τυχαίο αριθμό χαρακτήρων και τον μετατρέπει σε μια συμβολοσειρά με σταθερό αριθμό χαρακτήρων. Ακόμα και μια μικρή αλλαγή στην αρχική

κρυπταλγόριθμο. Η σύνοψη αυτή δημιουργείται εισάγοντας ένα οποιουδήποτε μεγέθους αρχικό κείμενο, το οποίο παράγει μια τιμή συγκεκριμένου μεγέθους. Η βασική αρχή αυτής της διαδικασίας είναι η μονοδρομικότητα της μετατροπής, δηλαδή να μην είναι δυνατή η εύρεση του αρχικού κειμένου, από την τιμή που έχει προκύψει ή τουλάχιστον να είναι υπερβολικά δύσκολο. Εκτός από τη δημιουργία της ψηφιακής υπογραφής, η συνάρτηση κατακερματισμού μπορεί να χρησιμοποιηθεί, για να ελεγχθεί η ακεραιότητα του αρχικού μηνύματος. Με αυτό τον τρόπο, όταν αποστέλλεται ένα μήνυμα και η σύνοψή του (hash), ο παραλήπτης μπορεί να εκτελέσει πάλι την συνάρτηση κατακερματισμού και να αντιπαραβάλει τις τιμές των δυο συνόψεων: αυτής που παρέλαβε με αυτή που υπολόγισε. Έτσι, μπορεί να εξασφαλιστεί ότι δεν έχει παρεμβληθεί κάποιος τρίτος ανάμεσα στον αποστολέα και τον παραλήπτη που να έχει κάνει οποιαδήποτε αλλαγή στο μήνυμα, γιατί αν το έκανε αυτό, θα ανιχνευθεί με την αντιπαραβολή των συνόψεων.

6.4 Η απόκρυψη της ταυτότητας των υποκειμένων

6.4.1 Ο νομικός χαρακτήρας της ψευδωνυμοποίησης και της ανωνυμοποίησης

Πέραν της κρυπτογράφησης σύμφωνα με τον ΓΚΠΔ, το άρθρο 32 ορίζει ότι και η ψευδωνυμοποίηση δύναται να διασφαλίσει το κατάλληλο επίπεδο ασφάλειας στα δεδομένα προσωπικού χαρακτήρα έναντι των κινδύνων.

Άλλες σημαντικές αναφορές στην ψευδωνυμοποίηση στον Κανονισμό υπάρχουν στο άρθρο 40[132], όσον αφορά τις ενώσεις και άλλους φορείς που εκπροσωπούν υπευθύνους επεξεργασίας, στο άρθρο 89[133], όπου περιλαμβάνεται μεταξύ των εγγυήσεων

συμβολοσειρά δημιουργεί ένα εντελώς νέο hash. Η αντίστροφή μαθηματική επίλυση δεν είναι εφικτή. Δηλαδή, αν κάποιος ξέρει το hash δεν μπορεί να βρει, ή να γνωρίζει το αρχικό κείμενο.

[132] Γίνεται αναφορά στην ψευδωνυμοποίηση, όπου ορίζεται ότι ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας παροτρύνονται να εκπονούν κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του κανονισμού ΓΚΠΔ όσον αφορά μεταξύ άλλων και την ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα.

[133] Στο άρθρο 89 («Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς») η ψευδωνυμοποίηση περιλαμβάνεται μεταξύ των εγγυήσεων ότι έχουν θεσπιστεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε (περαιτέρω) επεξεργασία για λόγους αρχειοθέτησης για λόγους γενικού συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

ότι έχουν θεσπιστεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα και στο άρθρο 25[134] όσον αφορά τις απαιτήσεις του νόμου για την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού.

Ο Κανονισμός ορίζει την τεχνική της ψευδωνυμοποίησης στο άρθρο 4 παρ. 5, ότι: «ψευδωνυμοποίηση είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τέτοιο 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». Με την ψευδωνυμοποίηση αντικαθίσταται η ταυτότητα δηλαδή του υποκειμένου των δικαιωμάτων, με τρόπο που να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώρισή του.

Στο πλαίσιο του ΓΚΠΔ τα ανωνυμοποιημένα και τα ψευδωνυμοποιημένα δεδομένα, αντιμετωπίζονται ως δύο εντελώς διαφορετικές κατηγορίες. Η ανωνυμοποίηση και ο περιορισμός των δεδομένων, συνιστούν σημαντικές πλευρές των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας[135]. Ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων[136]. Απαραίτητη προϋπόθεση είναι ασφαλώς, τα δεδομένα να έχουν συλλεχθεί σύμφωνα με τη νομοθεσία των προσωπικών δεδομένων και η αποθήκευσή τους γίνεται με τρόπο που είναι αναγνώσιμα σε απλή μορφή. Η επεξεργασία επιπλέον, πρέπει να είναι σύμφωνη με τις οδηγίες που έχουν τεθεί από την Γνώμη 3/2013 της Ομάδας του άρθρου 29[137]. Αυτό σημαίνει ότι η νομική βάση της ανωνυμοποίησης μπορεί να βρεθεί στα

[134] Στην προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού, ορίζεται ότι: «ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση».

[135] Λ. Μήτρου, Privacy by Design Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔΙΤΕ (π. ΔΙΜΕΕ), τεύχος 1/2013, κεφ. Οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

[136] Λαμπρινουδάκης Κ., Γκρίτζαλης Σ., Μήτρου Λ., Κάτσικας Σ., «Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών», εκδ. Παπασωτηρίου. 2010

[137] Γνώμη 3/2013 της επιτροπής του άρθρου 29, όσον αφορά τον περιορισμό του σκοπού της επεξεργασίας.

πλαίσια του άρθρου 7 της Οδηγίας e-Privacy[138], εφόσον πληρούνται οι προϋποθέσεις του άρθρου 6 της Οδηγίας.

Κατά συνέπεια, ανωνυμοποιώντας τα δεδομένα καθίσταται θεωρητικά αδύνατο να προσδιοριστεί το υποκείμενο των δεδομένων, σε αντίθεση με την τεχνική της ψευδωνυμοποίησης με την οποία δεν διαγράφεται η ταυτότητα, αλλά αντικαθίσταται με τέτοιο τρόπο, ώστε να απαιτούνται επιπλέον πληροφορίες για να είναι δυνατή η αναγνώριση των αρχικών υποκειμένων. Συνεπώς, βάσει και της αιτ. σκέψης (26)[139], ο ΓΚΠΔ δεν εφαρμόζεται σε τέτοιου είδους ανωνυμοποιημένες πληροφορίες, αφού δεν μπορούν να συσχετιστούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα[140].

6.4.2 Η τυχαιοποίηση ως τεχνική ανωνυμοποίησης

Ο σκοπός της ανωνυμοποίησης είναι να αποτρέψει την δυνατότητα συσχέτισης των δεδομένων με την ταυτότητα των υποκειμένων που τους ανήκουν. Υπάρχουν διάφορες τεχνικές ανωνυμοποίησης, οι οποίες μπορούν να εξυπηρετήσουν τον σκοπό της προστασίας των προσωπικών δεδομένων, αλλά δεν υπάρχει κάποιο ορισμένο στάνταρ από την Ευρωπαϊκή Νομοθεσία για το ποιο είναι το επιθυμητό επίπεδο, ώστε να εξασφαλίζεται ότι υπάρχει ανωνυμοποίηση. Από τον ορισμό της νομοθεσίας ότι πρέπει ο υπεύθυνος «θεσπίσει τα κατάλληλα τεχνικά και οργανωτικά μέτρα», γίνεται κατανοητό ότι ο νομοθέτης εννοεί όλα τα λογικά να χρησιμοποιηθούν στην περίσταση, ανάλογα με την παρούσα τεχνολογική εξέλιξη και κόστος εφαρμογής τους για τον εκάστοτε οργανισμό.

---

[138] Αναφορές στην e-Privacy Directive (Directive 2002/58/EC), άρθρο 6 παρ. 1 όπου ορίζει ότι: «1. Τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο δημόσιου δικτύου ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας.», άρθρο 9 παρ. 1: «Στις περιπτώσεις όπου δεδομένα θέσης εκτός των δεδομένων κίνησης, που αφορούν τους χρήστες ή συνδρομητές δικτύων ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, είναι δυνατό να υποστούν επεξεργασία, η επεξεργασία αυτή επιτρέπεται μόνον όταν αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση των χρηστών ή συνδρομητών στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας.» και αιτιολογική σκέψη 29: «…Δεδομένα κίνησης που χρησιμοποιούνται για εμπορική προώθηση υπηρεσιών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας θα πρέπει επίσης να εξαλείφονται ή να καθίστανται ανώνυμα έπειτα από την παροχή της υπηρεσίας…».

[139] Αναφέρονται ως πληροφορίες που δεν μπορούν να συσχετιστούν με 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.

[140] Βλ. Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου, Προσωπικά Δεδομένα: Νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους (Αθήνα: Αντ. Ν. Σάκκουλας, 2007), σελ. 33-34.

Δεν απαιτείται -ως εκ τούτου- κάποιος συγκεκριμένος τρόπος που να πιστοποιεί ότι δεν γίνεται να αναγνωριστούν τα υποκείμενα, αρκεί να είναι πιθανό ότι δεν γίνεται[141]. Συνεπώς, ακόμα και από τους ορισμούς, γίνεται κατανοητό ότι εμπεριέχεται ένα αποδεκτό επίπεδο κινδύνου και άρα πιθανή αποτυχία της ανωνυμοποίησης και ενδεχόμενη ταυτοποίηση, η οποία όμως δεν σημαίνει απαραίτητα ότι δεν είχαν ληφθεί τα κατάλληλα μέτρα από τον υπεύθυνο επεξεργασίας και ότι θα του καταλογιστεί η ευθύνη για την διαρροή των δεδομένων.

Στα πλαίσια προστασίας των προσωπικών δεδομένων, η τυχαιοποίηση (randomization), μπορεί να χρησιμοποιηθεί σαν εργαλείο ανωνυμίας μέσω της προσθήκης θορύβου ή της τυχαίας μετάθεσης των δεδομένων σε σύνολα δεδομένων (datasets) που πρόκειται να χρησιμοποιηθούν για διεξαγωγή ερευνών ή για στατιστικούς λόγους.

Η τυχαιοποίηση είναι ένα σύνολο τεχνικών που χρησιμοποιούνται, για να αλλάξουν την εγκυρότητα των στοιχείων με σκοπό να μειώσουν την σύνδεση μεταξύ δεδομένων και υποκειμένου. Η τυχαιοποίηση από μόνη της δεν αλλάζει την μοναδικότητα κάθε εγγραφής, δηλαδή τα δεδομένα της καθεμίας παραπέμπουν στο αρχικό υποκείμενο των δεδομένων, αλλά αλλάζοντας με χρήση αλγορίθμου ορισμένα μόνο δεδομένα της εγγραφής, παρέχεται ένα επίπεδο προστασίας ενάντια σε επιθέσεις «εξαγωγής συμπεράσματος» (Inference attacks)[142]. Ο τύπος αυτός επίθεσης, προσπαθεί να εξάγει συμπεράσματα για μία «ευαίσθητη» πληροφορία ενός ατόμου, ακόμα και αν δεν αναγνωρίζεται επακριβώς ποια είναι η καταχώρησή του στον ανωνυμοποιημένο πίνακα.

Η ανωνυμία με τυχαιοποίηση συνήθως επιτυγχάνεται προσθέτοντας «θόρυβο» στα δεδομένα, για να αποκρυφθεί η ταυτότητα του υποκειμένου. Με την διαδικασία αυτή αλλοιώνονται τυχαία κάποια απ' τα στοιχεία κάθε εγγραφής, τηρώντας όμως την αναλογία των χαρακτηριστικών των αρχικών εγγραφών. Λχ. σε ιατρικό σύνολο δεδομένων, που έχει σκοπό να βρει την πιθανότητα εμφάνισης μιας ασθένειας βάσει μιας συγκεκριμένης υψηλής τιμής σε εξέταση αίματος, θα αλλάξουν τα μεμονωμένα δεδομένα της κάθε εγγραφής, αλλά στο σύνολό τους, η πιθανότητα εμφάνισης της ασθένειας με βάση το ύψος της τιμής θα παραμείνει ίδιο. Τα στοιχεία με αυτόν τον τρόπο φαίνονται σαν πραγματικά και δεν είναι εύκολη η σύγκριση των δεδομένων αυτών με δεδομένα άλλης λίστας, για να

[141] Γνώμη 5/2014 της επιτροπής του άρθρου 29, σελ.6
[142] Γνώμη 5/2014 της επιτροπής του άρθρου 29, σελ.12

εξαχθούν συμπεράσματα. Η τεχνική αυτή χρησιμοποιείται συνήθως σε συνδυασμό με άλλες.

Η τυχαιοποίηση μπορεί να επιτευχθεί και με την τεχνική της μετάθεσης (Permutation), κατά την οποία τα δεδομένα ανακατεύονται μεταξύ των μεμονωμένων εγγραφών. Από μόνη της η τεχνική αυτή επίσης δεν παρέχει επαρκές επίπεδο ασφάλειας, αλλά μπορεί να χρησιμοποιηθεί σε συνδυασμό με την «προσθήκη θορύβου», κατά την οποία επίσης διατηρείται η αναλογία των χαρακτηριστικών των αρχικών εγγραφών.

Η διαφοροποιημένη ιδιωτικότητα (Differential Privacy)[143], επίσης ανήκει στην κατηγορία της τυχαιοποίησης. Με αυτή δεν αλλάζει το αρχικό σύνολο δεδομένων, αλλά αντίθετα η πρόσβαση περιορίζεται στα απαραίτητα δεδομένα, ώστε να απαντηθεί συγκεκριμένο ερώτημα που γίνεται στην βάση δεδομένων και προστίθεται, πριν παραδοθεί το αποτέλεσμα, ένα επίπεδο «θορύβου», όσο απαιτείται κάθε φορά για να εγγυηθεί την ανωνυμία[144]. Η τεχνική αυτή θεωρείται η πιο σύγχρονη και ασφαλέστερη μέχρι τώρα, και χρησιμοποιείται από πολλές μεγάλες εταιρείες[145].

Μια σύγχρονη λύση για ανωνυμοποίηση είναι αυτή της ομομορφικής κρυπτογράφησης (Homomorphic encryption), η οποία επιτρέπει την επεξεργασία των αριθμητικών δεδομένων στην κρυπτογραφημένη τους μορφή, χωρίς δηλαδή να απαιτείται η ενδιάμεση αποκρυπτογράφησή τους (βλ. παρακάτω 6.4.4. Η κρυπτογράφηση ως τεχνική ψευδωνυμοποίησης).

6.4.3 Γενίκευση γνωρισμάτων

Η τεχνική της γενίκευσης των γνωρισμάτων αντίθετα, ακολουθεί διαφορετική προσέγγιση. Με αυτή μεταβάλλονται κατάλληλα οι τιμές των πεδίων που είναι ψευδοαναγνωριστικά, μέσω γενίκευσής τους (generalization)[146]. Δημοσιοποιείται δηλαδή για κάθε εγγραφή του συνόλου δεδομένων, ένα εύρος τιμής λχ. ύψους, κιλών και όχι συγκεκριμένες τιμές.

---

[143] Dwork, C. Differential privacy. In Automata, languages and programming, pp 1-12. Springer Berlin Heidelberg, 2006

[144] Βλ. Felten, Ed., Protecting privacy by adding noise., 2012, URL: https://techatftc.wordpress.com/2012/06/21/protecting-privacy-by-adding-noise/

[145] Εταιρίες που είναι γνωστό ότι τις χρησιμοποιούν είναι η Google, η Apple και η Uber, βλ. ενδεικτικά πολιτική ανωνυμοποιημένων δεδομένων της Google, https://policies.google.com/technologies/anonymization?hl=el

[146] Γνώμη 5/2014 της επιτροπής του άρθρου 29, σελ.16

Στην τεχνική αυτή απαιτείται να βρίσκεται η σωστή ισορροπία, καθώς μπορεί να επιτευχθεί η επιθυμητή ανωνυμοποίηση ανάλογα με το μέγεθος του εύρους που θα χρησιμοποιηθεί αλλά από την άλλη υπάρχει απώλεια χρήσιμων πληροφοριών που θα μπορούσαν να είναι χρήσιμες για την εξαγωγή συμπερασμάτων.

6.4.4 Η κρυπτογράφηση ως τεχνική ψευδωνυμοποίησης

Παρόλο που τα ψευδωνυμοποιημένα δεδομένα υπάγονται στις περιοριστικές διατάξεις του ΓΚΠΔ, ενδέχεται να μην απαιτείται ενημέρωση του υποκείμενου, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που το αφορούν, όταν τα δεδομένα αυτά είναι κρυπτογραφημένα[147].

Η κρυπτογράφηση σε αντίθεση με την ψευδωνυμοποίηση, καθιστά ολόκληρα τα δεδομένα «μη αναγνώσιμα» και όχι μόνο τα προσωπικά δεδομένα που εμπεριέχονται σε ένα σύνολο δεδομένων. Συνεπώς στην κρυπτογραφημένη τους μορφή είναι αδύνατο να χρησιμοποιηθούν για έρευνα ή στατιστική ανάλυση, ή να εξαχθεί οποιοδήποτε συμπέρασμα, αφού θα πρέπει να αποκρυπτογραφηθούν πρώτα, ώστε να βγάζουν κάποιο νόημα και γι' αυτό η απλή χρήση κρυπτογράφησης, δεν μπορεί να χρησιμοποιηθεί ως τεχνική ψευδωνυμοποίησης.

Παρόλα αυτά, έχουν αναπτυχθεί μέθοδοι που μπορούν να εκμεταλλευτούν τα πλεονεκτήματα την κρυπτογραφίας και να προσφέρουν ασφάλεια στην επεξεργασία ψευδωνυμοποιημένων δεδομένων. Αυτές οι μέθοδοι χρησιμοποιούνται κυρίως στον τομέα της μηχανικής μάθησης, όπου καθίσταται δυνατή η χρησιμοποίηση των δεδομένων αυτών.

Η κύρια μέθοδος που χρησιμοποιείται είναι αυτή της ομομορφικής κρυπτογράφηση (Homomorphic encryption), τεχνική που μπορεί να έχει εφαρμογές σε πολλές περιπτώσεις[148], η οποία αποτελεί μια μέθοδο ασύμμετρης κρυπτογραφίας και απαιτεί ένα ιδιωτικό κλειδί, για να αποκρυπτογραφηθεί.

Στα μαθηματικά ο όρος «ομομορφικό» αφορά τον μετασχηματισμό ενός συνόλου δεδομένων σε ένα άλλο διατηρώντας παράλληλα τις σχέσεις μεταξύ των στοιχείων και στα δύο σύνολα. Επειδή τα δεδομένα σε ένα ομομορφικό σύστημα κρυπτογράφησης

[147] Άρθρο 34 ΓΚΠΔ («Ανακοίνωση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα στο Υποκείμενο των Δεδομένων»)

[148] Garcia F.D., Jacobs B. (2011) Privacy-Friendly Energy-Metering via Homomorphic Encryption. In: Cuellar J., Lopez J., Barthe G., Pretschner A. (eds) Security and Trust Management. STM 2010. Lecture Notes in Computer Science, vol 6710. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22444-7_15, σελ. 226

διατηρούν την ίδια δομή, πανομοιότυπες μαθηματικές λειτουργίες, είτε αυτές εκτελούνται σε κρυπτογραφημένα ή σε μη κρυπτογραφημένα δεδομένα, θα οδηγήσουν σε ισοδύναμα αποτελέσματα.

Η διαφορά όμως είναι ότι επιτρέπει σε εξουσιοδοτημένους χρήστες να εκτελούν υπολογισμούς ενώ είναι ακόμα κρυπτογραφημένα, χωρίς δηλαδή να υπάρχει πρόσβαση στα προσωπικά δεδομένα που επεξεργάζονται. Με την χρησιμοποίηση αυτής της τεχνικής λχ. ένα νοσοκομείο θα μπορούσε να προστατεύσει προσωπικά δεδομένα ασθενών του, στέλνοντας στοιχεία ενός υποκειμένου για ανάλυση σε ένα απομακρυσμένο, μη συμμορφούμενο με τον Κανονισμό εργαστήριο ή σύστημα και να τα πάρει πίσω κρυπτογραφημένα. Η Intel προσφέρει εργαλεία εφαρμογής HE, για να βοηθήσει ερευνητές να αναπτύξουν νευρωνικά δίκτυα που μπορούν να λειτουργούν με κρυπτογραφημένα δεδομένα[149].

6.4.5 Προβλήματα στην χρήση τεχνικών ανωνυμοποίησης και επαναταυτοποίησης υποκειμένων.

Κατά την διαδικασία της ανωνυμοποίησης αφαιρούνται από τα δεδομένα όλες οι πληροφορίες που μπορούν να ταυτοποιήσουν το υποκείμενο των δεδομένων (όπως ονοματεπώνυμο, ημερομηνίες γέννησης κα.), διατηρώντας όμως όλα τα υπόλοιπα στοιχεία, ώστε τα δεδομένα αυτά να είναι χρήσιμα για έρευνα, όπως λχ. να μπορεί να γίνει εντοπισμός επαναλαμβανόμενων μοτίβων για εξαγωγή χρήσιμων συμπερασμάτων.

Όμως, ακόμα και αν δεν είναι προφανής η ταυτότητα του ανθρώπου στον οποίο αναφέρονται τα δεδομένα, πρέπει, για να χαρακτηριστούν ως ανώνυμα, να εξεταστεί πρώτα αν όντως έχει εκμηδενιστεί η δυνατότητα ανακάλυψης της ταυτότητας των υποκειμένων.

Η χρήση των ανωνυμοποιημένων δεδομένων βρίσκεται στο επίκεντρο πολλών νέων εφαρμογών στην ιατρική[150] ή και σε τεχνολογίες αιχμής όπως η τεχνητή νοημοσύνη (AI). Σύμφωνα όμως με έρευνα[151] που δημοσιεύθηκε, είναι σχεδόν αδύνατο να υπάρχει

[149] HE-Transformer for nGraph: Enabling Deep Learning on Encrypted Data, https://www.intel.ai/he-transformer-for-ngraph-enabling-deep-learning-on-encrypted-data/.

[150] Βλ. url: https://www.tovima.gr/2018/02/26/society/oplo-kata-twn-epidimiwn-ta-anwnymopoiimena-dedomena/ (τελευταία πρόσβαση 12-2-2021)

[151] Luc Rocher, Julien M. Hendrickx & Yves-Alexandre de Montjoye, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications, 2019

πραγματική ανωνυμοποίηση ιδίως σε μεγάλες βάσεις δεδομένων, μόνο με την διαγραφή προσωπικών στοιχείων.

Στο παρελθόν έχουν υπάρξει αρκετές περιπτώσεις, κατά τις οποίες ανώνυμα δεδομένα μπόρεσαν τα ταυτοποιηθούν (Netflix 2008, IMDB 2014 κα.)[152] αλλά ποτέ μέχρι τώρα καμία πρακτική δεν απέδιδε σίγουρα αποτελέσματα.

Ερευνητές του Πανεπιστημίου «Université catholique de Louvain» του Βελγίου και του «Imperial College» του Λονδίνου, κατάφεραν να φτιάξουν ένα μοντέλο που να υπολογίζει πόσο εύκολα μπορούν να ταυτοποιηθούν τυχαία δεδομένα. Χρησιμοποιώντας 15 σύνολα δεδομένων (dataset) κατοίκων ενός δήμου κατάφεραν να έχουν αποτελέσματα ταυτοποίησης σε ποσοστό 99,98%.

Τα αποτελέσματά τους δείχνουν ότι ακόμα και σε σύνολα δεδομένων, όπου έχουν εφαρμοστεί «βαριές» τεχνικές ανωνυμοποίησης, είναι σχεδόν αδύνατο να πληρούνται οι απαιτήσεις που έχει θέσει ο ΓΚΠΔ και πλέον τίθεται εν αμφιβόλω τόσο η καταλληλότητα των τεχνικών εργαλείων όσο και της νομικής επάρκειας των κανόνων που χρησιμοποιούνταν μέχρι τώρα για την ανωνυμοποίηση δεδομένων. Η έρευνα αλλά και ο αυξανόμενος ρυθμός περιστατικών πώλησης προσωπικών δεδομένων στο ίντερνετ αποδεικνύουν ότι στην πράξη η ανωνυμοποίηση σαν έννοια, όπως νοείται στον αλλά και σε νομοθετικά κείμενα άλλων Κρατών (λχ. CCPA), πρέπει να εξελιχθεί και να προσαρμοστεί στις νέες τεχνολογικές εξελίξεις.

Συνεπώς κατά την χρησιμοποίηση τεχνικών ανωνυμοποίησης οι υπεύθυνοι επεξεργασίας και ιδίως όσοι χρησιμοποιούν μεγάλα σύνολα δεδομένων για έρευνα, πρέπει να λαμβάνουν υπόψη ορισμένες πολύ σημαντικές παραμέτρους όπως ότι η ψευδωνυμοποίηση προστατεύει μόνο επιφανειακά την ταυτότητα των υποκειμένων των δεδομένων, καθώς είναι ευάλωτη σαν τεχνική σε επιθέσεις συσχέτισης και απομόνωσης. Σε κάθε περίπτωση τα ψευδωνυμοποιημένα δεδομένα δεν εκφεύγουν του νομικού πλαισίου προστασίας των προσωπικών δεδομένων.

Τα ανωνυμοποιημένα δεδομένα δεν είναι καθόλου απίθανο να μπορέσουν σε δεύτερο χρόνο να ταυτοποιηθούν με τα υποκείμενα των δεδομένων. Και σε κάθε περίπτωση, ακόμα κι αν δεν υπόκεινται στις υποχρεώσεις του ΓΚΠΔ, δεν είναι απόλυτο ότι δεν ισχύει άλλη νομοθεσία, η οποία να επιβάλλει κανόνες στον χειρισμό τους, όπως

[152] Περίπτωση Netflix, url: https://www.independent.co.uk/life-style/gadgets-and-tech/news/netflix-hacked-recently-watched-fix-a6759336.html (τελευταία πρόσβαση 12-2-2021)

για παράδειγμα στις προϋποθέσεις αποθήκευσης και πρόσβασης στις πληροφορίες, όπως επιβάλει το άρθρο 5 παρ. 3 της Οδηγίας e-Privacy, βάση της οποίας έχουν εκδοθεί σειρές Νόμων στις Ευρωπαϊκές Χώρες, όπου επιβάλλεται η λήψη συναίνεσης από τα υποκείμενα των δεδομένων.

Κίνδυνος υπάρχει επίσης απ' το να μην συνεκτιμώνται οι επιπτώσεις στα υποκείμενα των δικαιωμάτων, ιδίως σε περιπτώσεις «κατάρτισης προφίλ»[153]. Ακόμα κι αν λόγω ανωνυμοποίησης δεν εφαρμόζονται οι νόμοι προστασίας προσωπικών δεδομένων, η χρήση ανωνυμοποιημένων συνόλων δεδομένων από τρίτους, δημιουργεί αυξημένο κίνδυνο να ταυτοποιηθούν τα υποκείμενα, καθώς, όταν γίνονται δημόσια, είναι ευκολότερη η αντιπαράθεση των δεδομένων τους και γίνεται δυνατή, έστω και εμμέσως, η λήψη αποφάσεων βάσει των διαπιστώσεων αυτών. Γι αυτό είναι πολύ σημαντική η εφαρμογή της αρχής του περιορισμού του σκοπού και να ληφθεί υπόψη η έννομη σχέση των υποκειμένων με τον υπεύθυνο επεξεργασίας, όπως και να εφαρμόζονται πάντα οι νόμιμες υποχρεώσεις συμμόρφωσης και διαφάνειας ως προς τον τρόπο επεξεργασίας των δεδομένων.

Στο επόμενο κεφάλαιο θα γίνει προσπάθεια ανάλυσης των βασικών αρχών της τεχνολογίας blockchain, των διαφοροποιήσεών του και έρευνα του νομικών πτυχών της τεχνολογίας, όπως και των έξυπνων συμβολαίων και του τρόπου που μπορεί σαν τεχνολογία να προστατεύσει τα προσωπικά δεδομένα.

[153] Βλ. αιτιολογική σκέψη 71 ΓΚΠΔ

7 ΤΟ ΠΑΡΑΔΕΙΓΜΑ ΤΟΥ BLOCKCHAIN

7.1 Εισαγωγή

Μία από τις ταχύτατα αναπτυσσόμενες τάσεις στην τεχνολογία του μέλλοντος, είναι και οι τεχνολογίες Blockchain. Οι τεχνολογίες blockchain μετασχηματίζουν ριζικά τον τρόπο οργάνωσης λειτουργίας της οικονομίας καθώς δημιουργούν την τεχνολογική δυνατότητα για ύπαρξη κατανεμημένης μορφής εμπιστοσύνης. Αυτό έχει τεράστια σημασία, καθώς μπορεί να επηρεάσει τις μέχρι σήμερα παραδοσιακές έμπιστες οντότητες (trusted authorities), τις συναλλαγές και τις ηλεκτρονικές υπηρεσίες.

Με τις τεχνολογίες blockchain, η εμπιστοσύνη που μέχρι τώρα υπήρχε λόγω μιας συμβατικής σχέσης δημιουργείται πλέον λόγω του κατανεμημένου και ασφαλούς τρόπου αποθήκευσης, διαχείρισης και ανταλλαγής πληροφορίας και διενέργειας ηλεκτρονικών συναλλαγών.

7.2 Τεχνολογίες Blockchain

Το Blockchain[154] είναι ένας κατανεμημένος λογιστικός κατάλογος ή αλλιώς καθολικό (distributed ledger), στον οποίο συναλλαγές ή δεδομένα συνδέονται μεταξύ τους σε μπλοκ δεδομένων, καθιστώντας τα πρακτικά αμετάβλητα και αδιαμφισβήτητα από όλους τους κατανεμημένους κόμβους (nodes) στους οποίους φυλάσσεται αντίγραφο καταλόγου. Έχει χαρακτηριστεί ως ένας συνδυασμός τεχνολογιών φύλαξης δεδομένων, εξασφάλισης μη μεταβλητότητας των δεδομένων και επίτευξης ομοφωνίας ως προς την πραγματική κατάσταση του καθολικού[155].

Η τεχνολογία του blockchain μπορεί να βρει εφαρμογή σε μια σειρά από κλάδους της οικονομίας και κοινωνίας και να αλλάξει τον τρόπο με τον οποίο λειτουργούν πολλά οικονομικά και επιχειρησιακά μοντέλα. Η κυριότερη χρήση της μέχρι τώρα ήταν στα ψηφιακά νομίσματα (bitcoin, ethereum κ.α.) αλλά επεκτείνεται και εφαρμόζεται ήδη και σε άλλους τομείς, όπως ενδεικτικά σε και άλλες χρηματοπιστωτικές / ασφαλιστικές υπηρεσίες, στην διακυβέρνηση, στη διαχείριση ψηφιακής ταυτότητας, στην τήρηση μητρώων, στην δημιουργία έξυπνων συμβολαίων (smart contracts), στη διαχείριση

[154] Βλ. https://el.wikipedia.org/wiki/Blockchain

[155] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M, 'On blockchain and its integration with IoT. Challenges and opportunities' [2018] Future Generation Computer Systems Elsevier BV, 88, σελ. 174

δικαιωμάτων πνευματικής ιδιοκτησίας, όπως και στο διαδίκτυο των πραγμάτων (IoT) ή στην διαχείριση εφοδιαστικής αλυσίδας.

Τα κύρια χαρακτηριστικά γνωρίσματα του blockchain είναι η διαφάνεια γιατί τα δεδομένα που περιέχει εμφανίζονται σε όλους τους συμμετέχοντες, ο καταμερισμός και η αποκέντρωση καθώς περισσότερα αντίγραφα του blockchain υπάρχουν ταυτόχρονα σε διαφορετικούς υπολογιστές, η αδυναμία μεταβολής, αφού μόλις εγγραφεί ένα δεδομένο, δε μπορεί στη συνέχεια να τροποποιηθεί ή να διαγραφεί και η απουσία διαμεσολάβησης γιατί κάθε απόφαση λαμβάνεται κατόπιν ομοφωνίας των συμμετεχόντων, χωρίς κεντρικό διαμεσολαβητή.

7.2.1 Ο τρόπος λειτουργίας του blockchain

Η θεμελιώδης διαφορά του blockchain από τα υφιστάμενα μητρώα και βάσεις δεδομένων είναι ότι για την τήρησή του δεν είναι αρμόδια μία κεντρική αρχή, αλλά οι λεγόμενοι κόμβοι (nodes) οι οποίοι, ενημερώνουν, ταυτόχρονα όλοι, το μητρώο για τις αλλαγές σε αυτό, ώστε πάντα να έχουν όλοι το ίδιο ακριβώς αντίγραφο. Αντί για παράδειγμα η τράπεζα μέσω του κεντρικού της συστήματος να επιβεβαιώνει τη μεταφορά χρημάτων ανάμεσα σε δύο άτομα, η επαλήθευση αυτή επιτυγχάνεται από τους κόμβους (χρήστες) με την τήρηση και ταυτόχρονη ενημέρωση του μητρώου από όλους χωρίς καμία κεντρική αρχή.

Με την επίτευξη συμφωνίας (consensus)[156] ανάμεσα στους όλους τους κόμβους δημιουργείται εμπιστοσύνη για την ορθότητα των στοιχείων που καταχωρούνται στο μητρώο. Όσο μεγαλύτερος είναι ο αριθμός των κόμβων που συμμετέχουν και τηρούν το μητρώο, τόσο μεγαλύτερος βαθμός εμπιστοσύνης και ακεραιότητας επιτυγχάνεται γιατί αν θέλει κάποιος να παραβιάσει τη βάση δεδομένων blockchain και να κάνει μη εξουσιοδοτημένες καταχωρήσεις θα πρέπει να παραβιάσει ταυτόχρονα όλους τους κόμβους που έχουν το αντίγραφο, κάτι σχετικά αδύνατο, σε αντίθεση με την τράπεζα του παραδείγματος, η οποία μπορεί να έχει μεγαλύτερη ασφάλεια αλλά χρειάζεται να γίνει μόνο μια παραβίαση του συστήματός της. Επιπλέον, προκειμένου να είναι λειτουργική μία δημόσια ή ανοιχτή βάση δεδομένων blockchain το δίκτυο των κόμβων πρέπει να έχει ένα

[156] Swanson T. 'Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems', 2015, https://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributedledger-systems (τελευταία πρόσβαση 5-2-2021).

κίνητρο για να θέλουν οι χρήστες να το διατηρούν κι επιπλέον θα πρέπει να συμφωνήσει να λειτουργεί σύμφωνα με δεοντολογικούς κανόνες.

Συνεπώς, το καθολικό σε μία πλατφόρμα blockchain δεν είναι μόνο αποκεντρωμένο (decentralized) αλλά και διανεμημένο (distributed) με την έννοια ότι ολόκληρο το μητρώο συναλλαγών τηρείται από όλους τους κόμβους και συγχρονίζεται ταυτόχρονα.

Το συνήθως ανοιχτό (open source) λογισμικό της κάθε πλατφόρμας blockchain καθορίζει τους όρους με τους οποίους θα καταχωρούνται τα δεδομένα στο μητρώο, τον τρόπο επαλήθευσής τους και φυσικά το είδος των πληροφοριών που θα καταχωρούνται. Επίσης, προσδιορίζει τις προϋποθέσεις και τον τρόπο δημιουργίας των καταχωρήσεων, για παράδειγμα στο bitcoin και γενικά στα κρυπτονομίσματα γίνεται μέσω συναλλαγής ή tokens. Αντίθετα η πλατφόρμα του ethereum[157] έχει τη δυνατότητα να ενσωματώσει και πιο σύνθετες πληροφορίες όπως τα λεγόμενα έξυπνα συμβόλαια (smart contracts) τα οποία γράφονται με διάφορες γλώσσες προγραμματισμού[158].

7.2.2 Διαφοροποιήσεις δικτύων blockchain

Για κάθε τομέα στον οποίο εφαρμόζονται οι τεχνολογίες blockchain απαιτούνται διαφορετικά επίπεδα αδειών από τους χρήστες. Η CNIL[159] έκανε μια κατηγοριοποίηση των ειδών στις κατηγορίες (α) των δημοσίων Blockchain δικτύων, τα οποία είναι προσβάσιμα σε οποιονδήποτε χρήστη. Σε αυτό κάθε πρόσωπο μπορεί να πραγματοποιήσει μια συναλλαγή, να συμμετάσχει στη διαδικασία επικύρωσης των «μπλοκ» ή να αποκτήσει ένα αντίγραφο του Blockchain, (β) στα Blockchain δίκτυα στα οποία η πρόσβαση απαιτεί άδεια, έχουν κανόνες που ορίζουν ποια πρόσωπα μπορούν να συμμετάσχουν στη διαδικασία επικύρωσης ή ακόμα και να πραγματοποιήσουν συναλλαγές και μπορούν, κατά

[157] Βλ. https://ethereum.org/en/ και το εργαλείο ανάπτυξης λογισμικού Ethereum Virtual Machine - EVM (https://ethereum.org/en/developers/docs/evm/) (τελευταία πρόσβαση 25-3-2021)

[158] Συνήθως με την Solidity (βλ. https://en.wikipedia.org/wiki/Solidity) αλλά και άλλες όπως η Vyper (https://vyper.readthedocs.io/) ή η bamboo (https://en.bitcoinwiki.org/wiki/Bamboo). Βλ. αναλυτικά A. Antonopoulos/G. Wood, Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media, Sebastopol, 2019, σελ. 127· M. Mukhopadhyay, Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, Packt Publishing, Birmingham, 2018, passim. (τελευταία πρόσβαση 25-3-2021)

[159] Βλ. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

περίπτωση, να έχουν πλήρη ή περιορισμένη πρόσβαση[160] και (γ) στα Blockchain δίκτυα τα οποία καλούνται «ιδιωτικά» και βρίσκονται υπό τον έλεγχο ενός χρήστη ο οποίος αποκλειστικά διασφαλίζει τον έλεγχο της συμμετοχής και της επικύρωσης[161]. Σύμφωνα με ορισμένους ειδικούς, οι εν λόγω χρήσεις δεν ακολουθούν τις κλασικές ιδιότητες του Blockchain, ιδίως την αποκέντρωση και την καταμερισμένη επικύρωση. Σε κάθε περίπτωση, δεν εγείρουν κάποιο συγκεκριμένο ζήτημα ως προς τη συμβατότητά τους με τον ΓΚΠΔ, καθώς πρόκειται απλώς για «κλασικές» βάσεις διανεμημένων δεδομένων.

Η CNIL, διαχωρίζει τους χρήστες των δικτύων blockchain σε τρία διαφορετικά είδη. Αυτά είναι (α) οι «έχοντες πρόσβαση» (accessors) οι οποίοι έχουν δικαίωμα ανάγνωσης και απόκτησης αντιγράφου της αλυσίδας, (β) οι «συμμετέχοντες» (participants), οι οποίοι έχουν δικαίωμα ανάγνωσης (η δημιουργία μίας συναλλαγής την οποία θέτουν προς επικύρωση) αλλά όχι απόκτησης αντιγράφου και (γ) οι «εξορύκτες» (miners), οι οποίοι επικυρώνουν μία συναλλαγή και δημιουργούν τα «μπλοκ» εφαρμόζοντας τους κανόνες του Blockchain, προκειμένου να γίνουν «αποδεκτοί» από την κοινότητα που απαρτίζει το κάθε δίκτυο blockchain.

7.2.3 Εφαρμογές της τεχνολογίας του blockchain

Οι κυριότερες χρήσεις της τεχνολογίας του blockchain σήμερα είναι στο χρηματοοικονομικό πεδίο με την ανάπτυξη των κρυπτονομισμάτων, αλλά και πιο πρόσφατα με την ανάπτυξη των έξυπνων συμβολαίων (smart contracts).

7.2.3.1 Κρυπτονομίσματα και bitcoin

Τα αποκεντρωμένα ψηφιακά νομίσματα, όπως και άλλα αντίστοιχά τους που επινοήθηκαν κατά καιρούς, λ.χ. μητρώα ακινήτων, υπάρχουν σαν έννοιες εδώ και πολύ καιρό, αλλά ποτέ μέχρι πρόσφατα δεν είχαν εξελιχθεί σε σημείο να αποτελέσουν ένα βιώσιμο εμπορικό προϊόν. Η πρώτη μορφή τέτοιων νομισμάτων ήταν τα ανώνυμα e-cash πρωτόκολλα της δεκαετίας του 1980 και 1990, τα οποία βασιζόντουσαν κυρίως σε μια πρώιμη μορφή κρυπτογραφίας γνωστή και ως τυφλή υπογραφή[162]. Η ιδέα της δημιουργίας νομισμάτων μέσω της επίλυσης υπολογιστικών προβλημάτων όπως και η ιδέα της

[160] Βλ. Sachin Shetty, Charles A. Kamhoua, Laurent L. Njilla, Blockchain for Distributed Systems Security, Wiley 2019, κεφ. Permissioned and Permissionless Blockchains, σελ. 193
[161] Βλ. για διαχωρισμό δημοσίων από ιδιωτικών δικτύων και Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M, 'On blockchain and its integration with IoT. Challenges and opportunities' [2018] Future Generation Computer Systems Elsevier BV, 88, σελ. 174
[162] Βλ.. https://en.wikipedia.org/wiki/Blind_signature (τελευταία πρόσβαση 25-3-2021)

αποκεντρωμένης συναίνεσης, προτάθηκαν πρώτη φορά το 1998 από τον μηχανικό υπολογιστών Wei Dai με την πρότασή του για τα b-money[163], ιδέα που δεν συνεχίστηκε η ίδια, αλλά αποτέλεσε την βάση για επόμενες προσπάθειες δημιουργίας ψηφιακών νομισμάτων που εν τέλει οδήγησε στην δημιουργία του bitcoin[164].

Το Bitcoin, συχνά συγχέεται σαν έννοια με το blockchain, αφού ήταν ουσιαστικά η πρώτη διαδεδομένη εφαρμογή της τεχνολογίας αυτής σε εμπορικό προϊόν. Δημιουργήθηκε από τον Satoshi Nakamoto, ο οποίος παραμένει ακόμα και σήμερα άγνωστο αν είναι υπαρκτό πρόσωπο ή ομάδα ανθρώπων. Το bitcoin συνδυάζει τεχνική κρυπτογραφίας με δημόσιο κλειδί με ένα αλγόριθμο συναίνεσης για την απόδειξη του ιδιοκτήτη των νομισμάτων. Αφού συγκεντρωθεί ένας αριθμός συναλλαγών, όλες μαζί εντάσσονται σε ένα block. Προκειμένου να «ολοκληρωθεί» ένα μπλοκ συναλλαγών και να ενταχθεί στην αλυσίδα των μπλοκ (blockchain), πρέπει να λυθεί ένας μαθηματικός γρίφος στο πλαίσιο μιας διαδικασίας επίτευξης ομοφωνίας, γνωστής ως proof of work[165]. Την εργασία αυτή αναλαμβάνουν οι λεγόμενοι «εξορύκτες» (miners)[166] οι οποίοι έχουν εγκατεστημένο το απαραίτητο λογισμικό και διαθέτουν εξοπλισμό εξαιρετικά μεγάλης υπολογιστικής ισχύος.

Καθώς η τήρηση του καθολικού περιλαμβάνει τη συσχέτιση των δεδομένων ενός μπλοκ με αυτά του προηγούμενου μπλοκ και αυτά με τη σειρά τους με του προηγούμενου κοκ, στην πραγματικότητα δημιουργείται μία αλυσίδα μπλοκ, η οποία φτάνει μέχρι το

---

[163] Βλ. https://en.bitcoin.it/wiki/B-money (τελευταία πρόσβαση 25-3-2021)

[164] Bambara J. Allen P., Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, McGraw-Hill Education, 2018, chapter 1.

[165] Στην πράξη το proof of work του bitcoin λειτουργεί ως εξής: το λογισμικό παράγει έναν αριθμό 256bit (hash target) ο οποίος εκπέμπεται στο δίκτυο και είναι κοινός για όλους τους miners. Ο γρίφος συνίσταται στο να βρεθεί ένας αριθμός hash του μπλοκ (header hash) ο οποίος είναι μικρότερος από τον αριθμό στόχο. Η εξεύρεση γίνεται και πάλι μέσω της διαδικασίας hashing, κατά την οποία λαμβάνονται υπόψη α) ο τελικός αριθμός hash που έχει προκύψει από την κρυπτογράφηση των συναλλαγών, β) ο αριθμός header hash του προηγούμενου block, γ) η ημερομηνία (time stamp) και δ) ένας αυθαίρετος αριθμός (nonce). Η λύση του γρίφου επιτυγχάνεται στην τύχη μόνο μέσω αλλεπάλληλων δοκιμών και αλλαγών του αριθμού nonce (ο οποίος είναι και η μόνη μεταβλητή) έως ότου προκύψει αποτέλεσμα του header hash μικρότερου του hash target. Όσο πιο μικρός είναι αυτός ο αριθμός στόχος (δηλαδή όσο περισσότερα είναι τα μηδενικά που προηγούνται) τόσο πιο μεγάλη είναι η δυσκολία εξεύρεσης του header hash. Η δυσκολία προσαρμόζεται συνεχώς, λαμβάνοντας υπόψη τη διαθέσιμη υπολογιστική ισχύ του των miners. Εναλλακτική μέθοδο σε άλλες πλατφόρμες blockchain αποτελεί η μέθοδος proof of stake, στην οποία η συμφωνία (consensus) για την επαλήθευση των μπλοκ από τους χρήστες επιτυγχάνεται με συνδυασμό άλλων κριτηρίων (όπως τον αριθμό των κρυπτονομισμάτων που έχει ο χρήστης που επαληθεύει το μπλοκ) και όχι με επίλυση γρίφου. Βλ. και https://en.wikipedia.org/wiki/Proof_of_work (τελευταία πρόσβαση 31-1-2021).

[166] Βλ. https://en.wikipedia.org/wiki/Bitcoin#Mining (τελευταία πρόσβαση 31-1-2021).

πρώτο μπλοκ, γνωστό ως genesis. Επομένως, οποιαδήποτε αναδρομική τροποποίηση σε μπλοκ της αλυσίδας θα επέφερε αλλαγές σε όλα τα επόμενα μπλοκ και τα δεδομένα τους, καθώς η τροποποίηση έστω κι ενός ελάχιστου δεδομένου μίας συναλλαγής παράγει έναν τελείως διαφορετικό hash, γεγονός που θα δημιουργούσε ανακολουθία στην αλυσίδα των μπλοκ.

7.2.3.2 Έξυπνα συμβόλαια

Έξυπνο συμβόλαιο ονομάζεται το πρόγραμμα (κώδικας) που αποθηκεύεται στο δίκτυο blockchain του Ethereum και εκτελείται για την πραγματοποίηση συγκεκριμένης συναλλαγής του τύπου «όταν συμβαίνει το Α, ενεργοποιείται η δράση Β».

Τα έξυπνα συμβόλαια μπορούν να περιγραφούν ως ένα σύνολο κωδικοποιημένων λειτουργιών που δεν προϋποθέτουν την ύπαρξη κάποιας αρχής, νομοθετικού πλαισίου ή τρόπους επιβολής των συμφωνηθέντων[167].

Μέσω της χρήσης της τεχνολογίας blockchain όχι μόνο καταργείται η ανάγκη για την ύπαρξη τρίτων μερών, αλλά εξασφαλίζεται ότι όλοι οι συμμετέχοντες γνωρίζουν τις λεπτομέρειες των συναλλαγών και ότι οι συμβατικοί όροι θα εκπληρώνονται αυτόματα όταν πληρωθούν ορισμένες προϋποθέσεις. Τα συμβαλλόμενα μέρη σε ένα έξυπνο συμβόλαιο μπορούν να διαπραγματεύονται τους βασικούς όρους των συναλλαγών, όπως προδιαγραφές των προϊόντων, ποσότητα, τίμημα, χρόνο και τόπο εκπλήρωσης μέσω της blockchain.

Όταν όλοι οι διασυνδεδεμένοι υπολογιστές του δικτύου επαληθεύσουν ότι πράγματι συνέβη μια συνδιαλλαγή, αυτή καθίσταται πλέον αδύνατο να αμφισβητηθεί. Κανένα από τα μέρη δεν χρειάζεται να εμπιστεύεται το άλλο για την εκτέλεση του συμβολαίου αλλά την ουδέτερη πλατφόρμα blockchain, η οποία θα εκτελεί τους σχετικούς συμβατικούς όρους όταν πληρωθούν οι προσυμφωνημένες προϋποθέσεις

Η εφαρμογή της νέας τεχνολογίας μπορεί να μειώσει τις δαπάνες και τους πιστωτικούς κινδύνους για τους δανειστές, καθώς η εκτέλεση των όρων των συμβολαίων θα γίνεται αυτοματοποιημένα και δεν θα υπάρχει κίνδυνος αθέτησής τους. Πράγμα που και αυτό με τη σειρά του μπορεί να βελτιώσει το κόστος των δανείων ή των συμβάσεων

[167] Βλ. S. Zoumpoulidis, Will Blockchain Technology, Smart Contracts & IoT be the new Lifeblood of Commerce?, Επιθεώρηση Δικαίου Πληροφορικής, κεφ. Α, και ISDA and Linklaters "Smart Contracts and Distributed Ledger – A Legal Perspective",10

που γίνονται με αυτό το τρόπο, αυξάνοντας παράλληλα το επίπεδο προστασίας και διαφάνειας.

7.3 Νομικές πτυχές της τεχνολογίας του Blockchain

Όπως είναι φυσιολογικό, η νέα αυτή τεχνολογία, ως ένας νέος τρόπος καταχώρησης και αποθήκευσης δεδομένων, θα πρέπει καταρχάς να εξεταστεί υπό το πρίσμα του δικαίου της προστασίας προσωπικών δεδομένων, ώστε να μπορεί να χρησιμοποιηθεί νόμιμα και να έχει ευρεία αποδοχή. Η απαίτηση χρήσης του ΓΚΠΔ όσον αφορά τεχνολογικές εφαρμογές βασισμένες σε blockchain, πρέπει να κρίνεται ανά περίπτωση και δεν γίνεται να υπάρχουν γενικές αναφορές ως προς την επιβεβλημένη εφαρμογή άρθρων του ΓΚΠΔ σε συγκεκριμένες λειτουργίες του blockchain, λόγω της περιπλοκότητας του συστήματος αλλά και λόγω του ότι δεν υπάρχει ανάγκη να εφαρμοστούν έλεγχοι πάντα, όταν τα δεδομένα δεν είναι ταυτοποιήσιμα.

Από άποψη εδαφικότητας, θα πρέπει πρώτα να καθοριστεί υπό ποιες προϋποθέσεις εφαρμόζεται η Ευρωπαϊκή νομοθεσία. Τέτοιες είναι οι περιπτώσεις που υπάγονται στο άρθρο 3 του ΓΚΠΔ, όπως η επεξεργασία δεδομένων υποκειμένων κατοίκων Ευρωπαϊκής Ένωσης μέσω της τεχνολογίας blockchain ή με άλλους τρόπους, σε οποιοδήποτε μέρος του κόσμου. Άλλη περίπτωση εφαρμογής του Κανονισμού μπορεί να είναι επίσης, όταν η επεξεργασία προσωπικών δεδομένων λαμβάνει χώρα στα πλαίσια κατάρτισης αρχείου συμπεριφοράς, για γεγονότα πάντα που έχουν γίνει στην Ευρώπη και υπάγονται στον ΓΚΠΔ.

Προβληματική μπορεί επίσης να γίνει η αναζήτηση της αρμόδιας Αρχής Προστασίας Προσωπικών Δεδομένων της Ευρωπαϊκής Ένωσης, καθώς είναι δύσκολο να προσδιοριστεί η «κύρια εγκατάσταση» όπως επιτάσσει το άρθρο 56 του ΓΚΠΔ. Όσον αφορά τα ιδιωτικά δίκτυα blockchain, η αρμόδια Αρχή μπορεί να καθοριστεί ως αυτή της κύριας έδρας του υπεύθυνου επεξεργασίας, που είναι συνήθως το νομικό πρόσωπο που λειτουργεί το δίκτυο ή έχει πρόσβαση στις υποδομές του. Για τα δημόσια (με άδεια ή χωρίς) μπορεί να είναι ιδιαιτέρως δύσκολο να καθοριστεί η «κύρια εγκατάσταση» καθώς ιδίως στα δημόσια χωρίς άδεια δίκτυα blockchain, απουσιάζει εντελώς κάποιο πρόσωπο που να θεωρείται κεντρικό και να έχει έλεγχο του δικτύου. Σε αυτές τις περιπτώσεις η

μόνη «λειτουργική» λύση θα ήταν να αναζητείται ο τόπος που έγινε η κάθε συγκεκριμένη επεξεργασία για την οποία τίθεται το ζήτημα της παραβίασης του ΓΚΠΔ[168].

Πολλά άλλα ερωτήματα μπορούν να προκύψουν στην εφαρμογή της Νομοθεσίας των προσωπικών δεδομένων σε εφαρμογές blockchain, όπως ποιος θα θεωρείται ο υπεύθυνος της επεξεργασίας και ποιος ο εκτελών την επεξεργασία. Ερωτήματα που είναι δύσκολο να απαντηθούν κυρίως σε ανοιχτές δημόσιες (χωρίς άδεια – permissionless) πλατφόρμες blockchain. Αλλά και σε θέματα άσκησης δικαιωμάτων μπορούν να προκύψουν πολλά προβλήματα, ιδίως όπως στην άσκηση του δικαιώματος διαγραφής ή ενημέρωσης των προσωπικών δεδομένων, στην οποία είναι εξαιρετικά αμφίβολο- αν και με ποιο τρόπο- γίνεται να ικανοποιηθούν σε μία βάση δεδομένων η οποία τηρείται ταυτόχρονα σε χιλιάδες αντίτυπα και στην οποία είναι αδύνατον να τροποποιηθούν, πόσο μάλλον να αφαιρεθούν δεδομένα και μάλιστα με τον τρόπο που απαιτεί ο ΓΚΠΔ.

7.3.1 Προσωπικά δεδομένα στο blockchain

Το Blockchain σαν τεχνολογία, μπορεί να αξιοποιηθεί σε μια πληθώρα εφαρμογών που αφορά προσωπικά δεδομένα, όπως στην μεταφορά περιουσιακών στοιχείων (π.χ. Bitcoin ή μετοχές), ως μητρώο το οποίο διασφαλίζει μία ανιχνευσιμότητα (π.χ. πιστοποιητικά διπλωμάτων) ή ακόμα να αξιοποιηθεί για την διεκπεραίωση ενός «έξυπνου συμβολαίου» (smart contract).

Ακόμα και αν όλοι οι τομείς στους οποίους μπορεί να εφαρμοστεί η τεχνολογία Blockchain δεν αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρακτικά, πολλές χρήσεις αυτής της τεχνολογίας απαιτούν την επεξεργασία προσωπικών δεδομένων, τόσο στο επίπεδο του περιεχομένου όσο και στο επίπεδο των πληροφοριών που σχετίζονται με τους συμμετέχοντες.

Επί της ουσίας, ένα Blockchain μπορεί να περιέχει δύο κατηγορίες δεδομένων προσωπικού χαρακτήρα:

- την ταυτοποίηση των συμμετεχόντων και των δευτερευόντων χρηστών: κάθε συμμετέχων/δευτερεύων χρήστης διαθέτει ένα δημόσιο κλειδί, το οποίο επιτρέπει την εξακρίβωση της ταυτότητας του αποστολέα και του παραλήπτη μίας συναλλαγής.

[168] Υπόθεση C-131/12 Google Spain [2014] EU:C:2014:317.

- τα συμπληρωματικά δεδομένα, τα οποία εγγράφονται «μέσα» σε μία συναλλαγή (π.χ. δίπλωμα, μετοχή). Στην περίπτωση που αυτά τα δεδομένα αποδίδονται σε φυσικά πρόσωπα, ενδεχομένως άλλα από τους συμμετέχοντες, άμεσα ή έμμεσα ταυτοποιήσιμα, πρόκειται για προσωπικά δεδομένα.

Βάσει αυτής της διάκρισης, εφαρμόζεται το πλαίσιο της συνήθους ανάλυσης του ΓΚΠΔ: ταυτοποίηση του υπεύθυνου της επεξεργασίας, σεβασμός δικαιωμάτων, εφαρμογή κατάλληλων εγγυήσεων, υποχρέωση ασφάλειας, κλπ. Όσον αφορά την κατηγοριοποίηση των χρηστών, οι μελέτες που πραγματοποίησε η CNIL οδήγησαν στο συμπέρασμα ότι, σε πολλές περιπτώσεις, ο συμμετέχων (το πρόσωπο που αποφασίζει για την εγγραφή ενός δεδομένου στο Blockchain) θα μπορούσε να θεωρηθεί ως ένας υπεύθυνος επεξεργασίας στο βαθμό που αποφασίζει για το σκοπό και τα μέσα της επεξεργασίας των δεδομένων.

Αναφορικά με την άσκηση των δικαιωμάτων, ορισμένα δικαιώματα μπορούν να ασκηθούν αποτελεσματικά, όπως το δικαίωμα πρόσβασης και το δικαίωμα φορητότητας. Όσον αφορά τα δικαιώματα διαγραφής - «στη λήθη», διόρθωσης και εναντίωσης στην επεξεργασία, δεν υπάρχει κάποια σαφής άποψη αλλά προκρίνεται η λύση ότι η κάθε περίπτωση θα πρέπει να αξιολογείται ξεχωριστά. Οι λύσεις αυτές, χωρίς να μπορούν να οδηγήσουν σε αυστηρά παρόμοια αποτελέσματα, συμβάλλουν στην εκπλήρωση των απαιτήσεων συμμόρφωσης με τον ΓΚΠΔ, ιδίως, περιορίζοντας την πρόσβαση σε συγκεκριμένα δεδομένα του επιλεγμένου μορφότυπου, όπως με κρυπτογράφηση, αποτύπωμα το οποίο έχει εκδοθεί από μία συνάρτηση κατακερματισμού (hash function). Η συμμόρφωσή με τον GDPR είναι λοιπόν ένα ζήτημα που θα πρέπει να ελεγχθεί. Σε γενικές γραμμές, όπως είναι κοινώς αποδεκτό, είναι προτιμότερο να αποφεύγεται η αποθήκευση μη κρυπτογραφημένων προσωπικών δεδομένων στο Blockchain.

7.3.2 Ενίσχυση της αρχής της λογοδοσίας (accountability)

Κάθε χρήστης, υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία, οφείλει βάσει του ΓΚΠΔ να είναι σε θέση να αποδεικνύει ότι είναι συμμορφωμένος με τον Κανονισμό σε κάθε πράξη επεξεργασίας που κάνει. Σε ορισμένες περιπτώσεις η χρήση της τεχνολογίας του blockchain μπορεί να προσφέρει πρακτικές λύσεις σε κάποια θέματα επεξεργασίας προσωπικών δεδομένων.

Η μονιμότητα των ενεργειών που πραγματοποιούνται στο Blockchain εκτός από την τα ενδεχόμενα προβλήματα που μπορεί να δημιουργήσει ως προς τον τρόπο

εφαρμογής της νομοθεσίας, μπορεί να δημιουργήσει παράλληλα και νέες δυνατότητες ενίσχυσης των αρχών του ΓΚΠΔ. Η αδυναμία μεταγενέστερης τροποποίησης του δημόσιου καταλόγου (ledger) δίνει την δυνατότητα δημιουργίας συστημάτων, τα οποία θα μπορούν να παρέχουν λύσεις στις υποχρεώσεις για την παροχή συγκατάθεσης με δυνατότητα ιχνηλασιμότητας, όπου παρατηρείται η μεγαλύτερη δυσκολία στην εφαρμογή του ΓΚΠΔ.

Στην σχεδίαση τέτοιων συστημάτων θα πρέπει να δίνεται η δυνατότητα στα υποκείμενα των δικαιωμάτων να χρησιμοποιήσουν μια έμπιστη και διαφανή λύση ώστε να μπορούν να παρακολουθούν τους υπεύθυνους και τους εκτελούντες την επεξεργασία που αποκτούν πρόσβαση άμεσα ή έμμεσα στα προσωπικά τους δεδομένα. Έπειτα, θα μπορούν να επαληθεύσουν ότι τα δεδομένα τους διαβάζονται, χρησιμοποιούνται και διαβιβάζονται χωρίς να παραβιάζεται η συναίνεσή τους. Τους παρέχεται με αυτό τον τρόπο η δυνατότητα να ανακαλέσουν την συγκατάθεσή τους, όποτε το επιθυμούν σε περίπτωση που αλλάξουν γνώμη ή έχει υπάρξει παρερμηνεία των συνθηκών υπό τις οποίες γίνεται η επεξεργασία των δεδομένων τους. Η προοπτική χρήσης ενός τέτοιου συστήματος ενισχύει την εμπιστοσύνη και την διαφάνεια στην λογοδοσία των προσωπικών δεδομένων όπως και προσφέρει την δυνατότητα ιχνηλασιμότητας των δεδομένων, με τρόπο που σέβεται την ιδιωτικότητα, χωρίς να αυξάνεται μαζί και ο κίνδυνος περαιτέρω έκθεσης των υποκειμένων, όταν αυτοί ζητούν την ανάκληση της συναίνεσης. Για τους υπεύθυνους επεξεργασίας επίσης η εφαρμογή ενός τέτοιου συστήματος, παρέχει ένα τρόπο σε αυτούς να αποδείξουν ότι έχουν πάρει συναίνεση από τα υποκείμενα των δεδομένων, ώστε να μπορούν να τα διατηρούν. Μια απ' τις πρακτικές εφαρμογές της εφαρμογής της αρχής της λογοδοσίας είναι στα έξυπνα συμβόλαια[169].

7.3.3 Νομικές πτυχές των έξυπνων συμβολαίων

Λόγω του ότι οι όροι και οι προϋποθέσεις σε μια γλώσσα προγραμματισμού, είναι σαφέστατα ορισμένες και γνωστές εκ των προτέρων, δεν υφίσταται με την χρήση έξυπνου συμβολαίου ούτε καν η μικρότερη αβεβαιότητα σχετικά με την ερμηνεία των όρων που υπάρχουν μέσα σε αυτό, σε αντίθεση με τα έγγραφα συμβόλαια, στα οποία δύο άνθρωποι μπορεί να αποδώσουν διαφορετικό νόημα στις ίδιες λέξεις. Συνεπώς, τα περιθώρια

[169] Neisse Ricardo, Steri Gary, Nai-Fovino Igor, A Blockchain-based Approach for Data Accountability and Provenance Tracking, 2017, ch.2

διαφορετικών ερμηνειών των συμβατικών όρων περιορίζονται σημαντικά (αν όχι εξαλείφονται) κατά την εκτέλεσή τους.

Από την άλλη πλευρά η τροποποίηση (λόγω π.χ. αλλαγών στο αναγκαστικού δικαίου νομοθετικό πλαίσιο που επήλθαν μετά την σύναψη του συμβολαίου) των όρων ενός έξυπνου συμβολαίου είναι δυσχερής, εφόσον έχει ενσωματωθεί σε πλατφόρμα blockchain. Η διασύνδεση των έξυπνων συμβολαίων με βάσεις δεδομένων (κρατικές ή ιδιωτικές) προκειμένου να ενημερώνονται αυτόματα με το ισχύον νομοθετικό πλαίσιο, και ο διαχωρισμός των όρων σε τροποποιήσιμους και μη, είναι μερικές από τις λύσεις που έχουν προταθεί[170].

Επίσης, λόγω της διασυνοριακής φύσης των συναλλαγών σε μία πλατφόρμα blockchain, σε ορισμένες περιπτώσεις θα είναι δύσκολο να εντοπιστούν τα χαρακτηριστικά εκείνα τα οποία θέτουν ως κριτήρια οι κανόνες ιδιωτικού διεθνούς δικαίου, όπως ο τόπος κατοικίας των μερών, ο τόπος κατάρτισης μίας σύμβασης, ο τόπος εκπλήρωσης, ώστε να προσδιοριστεί το εφαρμοστέο δίκαιο σε περίπτωση που αυτό δεν έχει συμφωνηθεί μεταξύ των συμβαλλόμενων μερών.

Τέλος, η πιο σημαντική νομική πτυχή από την εφαρμογή των έξυπνων συμβολαίων είναι αδιαμφισβήτητα το στάδιο της εκτέλεσης και κατά πόσο οι αυστηροί όροι αυτόματης εκπλήρωσης των συνεπειών σε βάρος του μη συμμορφούμενου μέρους συνάδουν με το δημόσιο χαρακτήρα των πράξεων εκτέλεσης. Αντίστοιχη είναι και η προβληματική στο πτωχευτικό δίκαιο, όπως για παράδειγμα πόσο νόμιμη θα ήταν η αυτόματη διακοπή λειτουργίας ενός αυτοκινήτου που χρησιμοποιεί ο οφειλέτης και πως θα μπορούσε να προστατευτεί ώστε να συνεχίσει να κάνει χρήση του αυτοκινήτου του, αν τεθεί σε καθεστώς πτωχευτικής ή προπτωχευτικής διαδικασίας κατά την οποία αναστέλλονται οποιεσδήποτε πράξεις εκτέλεσης κατά του οφειλέτη.

7.3.4 Νομικές πτυχές κρυπτονομισμάτων

Για την νομική τους αντιμετώπιση και τη συστηματική τους ένταξη στο αντίστοιχο σύνολο κανόνων δικαίου είναι απαραίτητος ο νομικός χαρακτηρισμός των κρυπτονομισμάτων. Παρά την ονομασία τους, η λειτουργία τους καθετί παρά παραπέμπει σε νομίσματα. Ένα ψηφιακό νόμισμα δεν είναι στην πραγματικότητα τίποτα περισσότερο από ένα νέο όρο που αναφέρεται σε μια μονάδα αξίας που εκδίδεται από μια ιδιωτική

[170] Raskin Max, The Law And Legality Of Smart Contracts, 2017, σελ. 309

οντότητα. Βασικό στοιχείο, όπως αναφέρθηκε παραπάνω, για την λειτουργία κάθε ανοιχτού πρωτοκόλλου blockchain, είναι η δημιουργία tokens του δικτύου αυτού, τα οποία είναι απαραίτητα για τη συμμετοχή στην κάθε πλατφόρμα δικτύου blockchain (σαν αυτό του Ethereum), όπως απαιτείται για παράδειγμα για την συμπλήρωση ενός έξυπνου συμβολαίου. Σύμφωνα με τον William Mougayar, συγγραφέα του "The Business blockchain"[171], ένα ψηφιακό νόμισμα είναι "μια μονάδα αξίας που δημιουργεί ένας οργανισμός για να αυτοδιοικήσει το επιχειρησιακό του μοντέλο και να ενδυναμώσει τους χρήστες του να αλληλεπιδράσουν με τα προϊόντα του, διευκολύνοντας παράλληλα τη διανομή και την κοινή χρήση των ανταμοιβών και των προνομίων για τους ενδιαφερόμενους". Ένα ψηφιακό νόμισμα είναι παρόμοιο με την έκδοση ενός τσεκ σε ψηφιακή μορφή. Ο κάτοχος του νομίσματος έχει το δικαίωμα να απαιτήσει το υποκείμενο περιουσιακό στοιχείο. Κάθε μεταβιβάσιμο περιουσιακό στοιχείο υλικό ή άυλο στοιχείο ή δικαίωμα, μπορούν να εκπροσωπούνται μέσω ψηφιακών tokens.

Επομένως, η φύση και η λειτουργία των κρυπτονομισμάτων προσιδιάζει περισσότερο σε ψηφιακά περιουσιακά στοιχεία, η αξία των οποίων είναι συνδεδεμένη και υπάρχει μόνο μέσα στο οικοσύστημα λειτουργίας ενός συγκεκριμένου πρωτοκόλλου blockchain (παρά σε νόμισμα). Η αξία δε αυτή καθορίζεται από τα τεχνικά χαρακτηριστικά του πρωτοκόλλου, τις λειτουργικές του δυνατότητες και εν τέλει την απήχησή και τη διάδοσή του στην κοινότητα στην οποία απευθύνεται.

Η έννοια των tokens μπορεί να γίνει πιο κατανοητή, αν δει κανείς την αρχιτεκτονική και τη δομή των εταιρειών που τα εκδίδουν και τα διαθέτουν, συνήθως μέσω αυτού που ονομάζεται Initial Coin Offering ή ICO (παραπέμποντας, μάλλον κατ' ευφημισμό, στο Initial Public Offering - IPO, δηλαδή τη δημόσια εγγραφή, με την οποία ουδεμία σχέση έχουν). Οι εταιρείες αυτές δημιουργούν υπηρεσίες, οι οποίες βασίζονται στην αποκεντρωμένη συν-δημιουργία, εξαρτώνται από την διάδοση των tokens και η βασική, αν όχι η μόνη, πηγή εσόδων είναι η αύξηση της αξίας των tokens ανάλογα με την επιτυχία της «οικονομίας» τους.

[171] Mougayar William, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley, 2016

7.4 Η Νομοθετική αντιμετώπιση από Ευρώπη και Ελλάδα

7.4.1 Το Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 3ης Οκτωβρίου 2018 σχετικά με τις τεχνολογίες κατανεμημένου καθολικού (DLT) και το σύστημα blockchain

Το Ευρωπαϊκό Κοινοβούλιο στις 3 Οκτωβρίου 2018, ενέκρινε ψήφισμά του σχετικά με τις «Τεχνολογίες κατανεμημένου καθολικού (DLT)[172]. Το Ψήφισμα υιοθετήθηκε για την προστασία και την ενίσχυση των πολιτών και των επιχειρήσεων της ΕΕ σε σχέση με συγκεκριμένα ζητήματα που ανακύπτουν αναφορικά με την τεχνολογία blockchain ή τεχνολογίες κατανεμημένου καθολικού (DLT), συμπεριλαμβανομένης της σχέσης με την προστασία δεδομένων προσωπικού χαρακτήρα και εν γένει με τον ΓΚΠΔ.

Το Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου περιλαμβάνει μεταξύ άλλων τις ακόλουθες βασικές συστάσεις:

- να πραγματοποιηθεί εμπεριστατωμένη ανάλυση του ισχύοντος νομικού πλαισίου των κρατών μελών όσον αφορά την εκτελεστότητα των έξυπνων συμβολαίων (smart contracts),
- να αναπτυχθούν τεχνικά πρότυπα για τις τεχνολογίες κατανεμημένου καθολικού,
- να αναπροσαρμοσθούν τα εξειδικευμένα προγράμματα σπουδών σε πανεπιστημιακό επίπεδο, ώστε να συμπεριλαμβάνονται οι σπουδές σε αναδυόμενες τεχνολογίες όπως η τεχνολογία κατανεμημένου καθολικού,
- οποιαδήποτε κανονιστική αντιμετώπιση της τεχνολογίας κατανεμημένου καθολικού θα πρέπει να είναι φιλοκαινοτόμος, να επιτρέπει μηχανισμό διαβατηρίου (passporting), και να διέπεται από τις αρχές της τεχνολογικής ουδετερότητας και της ουδετερότητας του επιχειρηματικού προτύπου,
- η Ευρωπαϊκή Επιτροπή και η Ευρωπαϊκή Κεντρική Τράπεζα να παράσχουν ενημέρωση για τις πηγές αστάθειας των κρυπτονομισμάτων, να εντοπίσουν τους κινδύνους για το κοινό και να διερευνήσουν τις δυνατότητες ενσωμάτωσης των κρυπτονομισμάτων στο ευρωπαϊκό σύστημα πληρωμών,
- ενθαρρύνεται η δημιουργία πολλών και ανθεκτικών κόμβων τεχνολογίας κατανεμημένου καθολικού προκειμένου να αποφευχθεί η συγκέντρωση

[172] Βλ. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_EL.html

δεδομένων στα χέρια λίγων φορέων της αγοράς που θα μπορούσε να οδηγήσει σε αθέμιτη σύμπραξη, και

- να διερευνηθούν περιπτωσιολογικές μελέτες χρήσης τεχνολογίας κατανεμημένου καθολικού στη διαχείριση των συστημάτων υγειονομικής περίθαλψης.

Το Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου αναγνωρίζει την ανάγκη συμμόρφωσης της τεχνολογίας blockchain με το ΓΚΠΔ και επισημαίνει τους κινδύνους που συνδέονται με την ιδιωτική ζωή και την προστασία των προσωπικών δεδομένων.

Υπογραμμίζει επίσης ότι σε ένα δημόσιο καθολικό (public ledger) τα δεδομένα είναι ψευδωνυμοποιημένα και όχι ανώνυμα. Αν και δεν είναι δυνατή η άμεση αναγνώριση των μεμονωμένων μελών σε ένα δίκτυο, είναι δυνατή η έμμεση αναγνώριση (μέσω αναγνωριστικών που συνδέονται με τα δεδομένα). Τα ψευδωνυμοποιημένα δεδομένα εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

Έτσι, το Ψήφισμα αναγνωρίζει ότι είναι «υψίστης σημασίας» να τηρείται κατά τη χρήση των τεχνολογιών κατανεμημένου καθολικού (DLT) η Ευρωπαϊκή νομοθεσία περί προστασίας των προσωπικών δεδομένων, ιδία δε ο ΓΚΠΔ, και καλεί την Επιτροπή και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων να προσφέρουν περαιτέρω καθοδήγηση στο θέμα αυτό.

Εντούτοις, φαίνεται ότι ζητήματα ιδιωτικότητας και προσωπικών δεδομένων μπορεί να προκύψει ότι συνιστούν σε ορισμένες περιπτώσεις ανυπέρβλητο εμπόδιο. Αν και η δυναμική περαιτέρω ανάπτυξης είναι σημαντική, είναι σαφές ότι τα πρότυπα του Γενικού Κανονισμού δεν είναι ευχερώς εφαρμόσιμα στην τεχνολογία blockchain.

7.4.2 Το Ευρωπαϊκό Παρατηρητήριο και η θέση της Ελλάδας

Ο σκοπός του Ευρωπαϊκού Παρατηρητηρίου και Φόρουμ για το Blockchain[173] είναι να παρακολουθεί τις πρωτοβουλίες όσον αφορά το blockchain στην Ευρώπη, να συσσωρεύσει ενδελεχή γνώση για το blockchain, να δημιουργήσει ένα τόπο συζήτησης με διαφάνεια και διαμοιρασμό πληροφοριών και απόψεων και να κάνει προτάσεις για τον ρόλο που μπορούσε να έχει η Ευρώπη στο blockchain. Πρόσφατα δημοσίευσε μια εκτενή μελέτη για την τρέχουσα κατάσταση του ευρωπαϊκού οικοσυστήματος blockchain[174]. Η

[173] Βλ. https://www.eublockchainforum.eu/
[174] Βλ.

μελέτη αναλύει την τρέχουσα κατάσταση τόσο για την υιοθέτηση όσο και για τη ρυθμιστική αντιμετώπιση των ψηφιακών προϊόντων (crypto assets) στην Ευρώπη.

Η Ελλάδα είναι συμβαλλόμενο μέρος του συνεταιρισμού του Ευρωπαϊκού Blockchain[175] και θεωρείται από την μελέτη ως αναδυόμενο οικοσύστημα blockchain για επιχειρήσεις και startups όπως και για κοινότητες με πρακτικές εφαρμογές. Το 2020 υπήρχαν τουλάχιστον 15 επιχειρήσεις που ασχολούνταν με τον τομέα του blockchain αποκλειστικά και με ανοδική τάση για περισσότερες. Οι επιχειρήσεις αυτές φαίνεται να ασχολούνται με όλο το εύρος των εφαρμογών του blockchain και όχι με κάποιο συγκεκριμένο τομέα ή σε συγκεκριμένη περιοχή. Η τεχνολογία του blockchain -όπως και τα ψηφιακά νομίσματα- δεν έχουν υιοθετηθεί από την Ελληνική Νομοθεσία και δεν υπάρχει καμία συγκεκριμένη αναφορά σε αυτά. Επίσης, διαπιστώνεται η έλλειψη κινήτρων υιοθέτησης και ενσωμάτωσης της τεχνολογίας σε επιχειρήσεις και ότι για την καθυστέρηση της υιοθέτησης της τεχνολογίας του blockchain -όπως και των ψηφιακών νομισμάτων- έπαιξε κρίσιμο ρόλο η κρίση χρέους των προηγούμενων ετών. Παρόλα αυτά, διαπιστώνεται ότι η Επιτροπή Κεφαλαιαγοράς και η Τράπεζα της Ελλάδος κάνουν προσπάθειες να το ενσωματώσουν στην Ελληνική έννομη τάξη και να προσφέρουν τελικά ένα ρυθμιστικό πλαίσιο για ψηφιακά προϊόντα.

7.4.3 Ελληνική νομοθεσία

Στην Ελλάδα, ο νέος Νόμος 4734/2020 (ΦΕΚ Α' 196/08.10.2020) με τίτλο «Τροποποίηση του ν. 4557/2018 (Α΄ 139) για την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας – Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας (ΕΕ) 2018/843[176] (L 156) και του άρθρου 3 της Οδηγίας (ΕΕ) 2019/2177 (L 334) και λοιπές διατάξεις», ενισχύει το νομικό πλαίσιο για την πρόληψη και καταπολέμηση του φαινομένου νομιμοποίησης εσόδων από παράνομες δραστηριότητες και χρηματοδότησης της τρομοκρατίας.

---

https://www.eublockchainforum.eu/sites/default/files/reports/_v01_0.pdf?utm_campaign=prgr&utm_medium=prgr&utm_source=link (τελευταία πρόσβαση 7-2-2021)

[175] Βλ. https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership (τελευταία πρόσβαση 7-2-2021)

[176] Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018L0843 (τελευταία πρόσβαση 21-5-2021)

Μια επίσης σημαντική αλλαγή είναι η επέκταση του πεδίου εφαρμογής του Νόμου 4557/2018, με απώτερο σκοπό να βελτιωθούν οι μηχανισμοί άμυνας του χρηματοπιστωτικού συστήματος και να περιοριστεί η ανωνυμία, που διέπει τα ψηφιακά νομίσματα και τις προπληρωμένες κάρτες.

Ως υπόχρεα πρόσωπα λογίζονται πλέον και κάθε πάροχος υπηρεσιών ανταλλαγής εικονικών νομισμάτων και παραστατικών νομισμάτων, όπως και κάθε πάροχος υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών.

Σημαντική είναι και η προσθήκη στο άρθρο 3 του Νόμου 4734/2020, όπου προστίθενται οι ορισμοί για το ηλεκτρονικό χρήμα, τα εικονικά νομίσματα και τους παρόχους υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών.

Μεταξύ άλλων, με την τροποποίηση του άρθρου 6 στον νέο Νόμο, ορίζεται ότι «η Επιτροπή Κεφαλαιαγοράς αναλαμβάνει εποπτικά καθήκοντα για τους παρόχους των υπηρεσιών ανταλλαγής εικονικών νομισμάτων και τους παρόχους υπηρεσιών θεματοφυλακής ψηφιακών πορτοφολιών».

Ο Νόμος εισάγει σοβαρούς ελέγχους σε διακρατικές συναλλαγές και πληρωμές με ηλεκτρονικό χρήμα ή με ειδική προπληρωμένη κάρτα, ακόμα και τις ανώνυμες που εκδίδουν άλλες χώρες στην Ευρώπη, περιορίζοντας αισθητά την ανωνυμία που υπήρχε στην διακίνηση χρημάτων μέσω κρυπτονομισμάτων.

Ουσιαστικά οι συναλλαγές που γίνονται μέσω πιστοποιημένων ιδρυμάτων δεν θα είναι ψευδωνυμοποιημένες, όπως ήταν μέχρι τώρα, αφού το ίδρυμα πλέον θα γνωρίζει και αν του ζητηθεί και το Κράτος, τα στοιχεία των ατόμων που κάνουν την συναλλαγή, πριν αυτή ψευδωνυμοποιηθεί από το εκάστοτε δίκτυο του κρυπτονομίσματος, καθώς ορίζεται ότι οι πελάτες θα πρέπει να αποδίδουν τα απαραίτητα στοιχεία, έτσι ώστε να είναι σε θέση να χρησιμοποιήσουν τις εν λόγω υπηρεσίες και τα στοιχεία θα μπορούν να δοθούν, εφόσον ζητηθούν, στις κατά νόμο διωκτικές και φορολογικές αρχές της εκάστοτε χώρας.

Συγκεκριμένα, όπως ορίζεται, παρέχεται πλέον η δυνατότητα στην εθνική Μονάδα Χρηματοοικονομικών Πληροφοριών (Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες) να έχει πρόσβαση σε μεγαλύτερο εύρος πληροφοριών κατά την άσκηση των καθηκόντων της. Επίσης, θεσπίζονται Μητρώα Τραπεζικών Λογαριασμών και Λογαριασμών Πληρωμών ως κεντρικό αυτοματοποιημένο μηχανισμό για την έγκαιρη πρόσβαση σε πληροφορίες σχετικά με την ταυτότητα των κατόχων τραπεζικών λογαριασμών και λογαριασμών πληρωμών και προβλέπεται στενότερη και πιο

συστηματική συνεργασία των αρχών προληπτικής εποπτείας και των αντίστοιχων αρχών εποπτείας για την καταπολέμηση του ξεπλύματος χρήματος, τόσο μεταξύ τους όσο και με τις αρμόδιες ευρωπαϊκές αρχές.

8 ΕΠΙΛΟΓΟΣ

8.1 Σύνοψη και συμπεράσματα

Η προστασία της ιδιωτικότητας των υποκειμένων, δεν είναι αυτοσκοπός των νομοθετημάτων που αφορούν την προστασία των προσωπικών δεδομένων. Προέκυψε από την διαχρονική ανάγκη των ατόμων να αποφεύγουν την επιτήρηση από τις νέες τεχνολογίες και η προστασία αυτή αποτελεί μια απ' τις ουσιαστικότερες εκφράσεις της δημοκρατίας σε κάθε πολίτευμα. Όσο προοδεύει η τεχνολογία, τόσο μεγαλύτερα γίνονται τα προβλήματα προστασίας της ιδιωτικότητας, καθώς αυτή έρχεται σε αντίθεση πολλές φορές με άλλα δικαιώματα ή συμφέροντα κρατικά ή ιδιωτικά. Κρίσιμο για την προστασία τους αποτελεί η ορθή εφαρμογή της αρχής της αναλογικότητας και η ορθή χρήση των κατάλληλων τεχνολογικών εργαλείων, ώστε να επιτυγχάνεται το επιθυμητό επίπεδο προστασίας σε κάθε περίπτωση. Για να επιτευχθεί αυτή η προστασία πρέπει τα νομοθετικά και τεχνολογικά εργαλεία να συμβαδίζουν, για να πετυχαίνουν το καλύτερο δυνατό αποτέλεσμα. Τα νομοθετικά κείμενα πρέπει να λαμβάνουν υπόψη συνεχώς τις νέες τεχνολογικές εξελίξεις και τα τεχνολογικά εργαλεία, όπως επίσης πρέπει να κρίνεται συνεχώς η αποδοτικότητα των χρησιμοποιούμενων μέτρων και τεχνικών. Τα τεχνολογικά εργαλεία ομοίως που χρησιμοποιούνται στον τομέα της ιδιωτικότητας, θα πρέπει να σχεδιάζονται με τρόπο που λαμβάνονται υπόψη εκ των προτέρων τα οριζόμενα από την εκάστοτε ισχύουσα νομοθεσία και όχι ανεξάρτητα μόνο με τεχνολογικά κριτήρια και έπειτα να γίνεται προσπάθεια να προσαρμοστούν στο νομικό καθεστώς. Η προσπάθεια αυτή, κωδικοποιήθηκε στον ΓΚΠΔ με την έννοια της ασφάλειας εκ του σχεδιασμού και εξ ορισμού. Ενώ υπάρχει πλέον μια βάση απ' την οποία μπορούν οι δύο αυτοί κλάδοι να συγκλίνουν και να προκύψουν νέες πρακτικές που σέβονται την ιδιωτικότητα, ο αντίκτυπος της έννοια αυτής είναι ακόμα περιορισμένος και κυρίως σε θεωρητικό επίπεδο χωρίς να έχει βρει κάποια διαδεδομένη πρακτική εφαρμογή.

Σε αυτή τη μελέτη έγινε μια προσπάθεια να γεφυρωθεί το νομικό και τεχνολογικό κενό όσον αφορά την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, μέσω της παράθεσης του νομοθετικού πλαισίου και των κρίσιμων τεχνολογιών που μπορούν να βοηθήσουν σε αυτό τον τομέα.

8.2 Μελλοντικές Επεκτάσεις

Οι τρόποι που μπορεί αυτή η μελέτη να επεκταθεί είναι πολλοί, καθώς το πλαίσιο προστασίας των προσωπικών δεδομένων στο σύγχρονο τεχνολογικό περιβάλλον είναι πολυεπίπεδο. Το πεδίο έρευνας είναι ευρύτατο και περιλαμβάνει την κάλυψη της ανάγκης προστασίας των δεδομένων με την χρήση νέων τεχνολογιών, όπως αυτών του διαδικτύου των πραγμάτων (IoT), της ανάλυσης μεγάλων δεδομένων (Big data analytics) και της τεχνητής νοημοσύνης (AI), που αρχίζουν να βρίσκουν πλέον εφαρμογή σε όλους τους τομείς της ζωής μας. Η μελέτη επίσης, μπορεί να κινηθεί προς την δημιουργία κανόνων σχεδιασμού για αυτές τις τεχνολογίες ξεκινώντας από την αρχή της προστασίας της ιδιωτικότητας, με σκοπό να γεφυρώσει τις επιστήμες της νομικής και της πληροφορικής στον τομέα αυτό, έτσι ώστε να δημιουργηθεί ένα κοινό πλαίσιο αναφοράς για όλους τους εμπλεκόμενους επαγγελματίες του τομέα.

Βιβλιογραφία στην Ελληνική Γλώσσα

Βιβλία

Αλεξανδροπούλου - Αιγυπτιάδου Ευγενία, Προσωπικά Δεδομένα, Εκδόσεις Νομική Βιβλιοθήκη, Θεσσαλονίκη, 2016

Αλεξανδροπούλου - Αιγυπτιάδου Ευγενία, Προσωπικά Δεδομένα: Νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους, Αθήνα: Αντ. Ν. Σάκκουλας, 2007

Βενιζέλος Ευάγγελος, Το Σύνταγμα του 1975/1986/2001, Εκδόσεις Αντ. Ν. Σάκκουλα, 2001

Γκριτζάλης Στέφανος, Γκριτζάλης Δημήτρης, Κατσίκας Σωκράτης, Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, 2003

Δαγτόγλου Πρόδρομος, Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα, Εκδόσεις Αντ. Ν. Σάκκουλας, 2012

Ιγγλεζάκης Δ. Ιωάννης, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679), εκδ. Interactive Books, (γ΄ εκδ.) 2020

Ιγγλεζάκης Δ. Ιωάννης, Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, Εκδόσεις Σάκκουλα, 2014

Ιγγλεζάκης Δ. Ιωάννης, Ευαίσθητα προσωπικά δεδομένα, Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων και οι συνέπειές της, ανατύπωση 2004, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2004

Ιγγλεζάκης Δ. Ιωάννης, Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου, Εκδόσεις Σάκκουλα, Αθήνα, Θεσσαλονίκη, 2003

Κανέλλος Λεωνίδας, The GDPR Handbook, 2020

Κότσαλης Λεωνίδας, Μενουδάκος Κωνσταντίνος, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων. Νομική διάσταση και πρακτική εφαρμογή, 2018

Λαμπρινουδάκης Κ., Γκρίτζαλης Σ., Μήτρου Λ., Κάτσικας Σ., «Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών», εκδ. Παπασωτηρίου. 2010

Μήτρου Λίλιαν, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων. Νέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα, εκδ. Σάκκουλα, 2017

Μήτρου Λίλιαν, Η δημοσιότητα της κύρωσης ή η κύρωση της δημοσιότητας, εκδ. Σάκκουλα, 2012

Παναγοπούλου-Κουτνατζή Φερενίκη, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία δεδομένων, εκδ. Σάκκουλα, 2017

Πλατής Ειρηνικός, Προσωπικά δεδομένα-Προστασία GDPR, Εκδόσεις Παπαδόπουλος, 2018

Ρούκουνας Εμμανουήλ, Διεθνής Προστασία των Ανθρωπίνων Δικαιωμάτων, Εκδόσεις Εστία, 1995

Τσαούσης Ν. Ηλίας, Τέσσερα αμφιλεγόμενα ζητήματα κατά την εφαρμογή του GDPR, ΕΠΙΧΕΙΡΗΣΗ, Τεύχος 174/2020, Οκτώβριος 2020

Χρυσόγονος Χ. Κώστας, Ατομικά και Κοινωνικά Δικαιώματα, 3η αναθεωρημένη έκδοση, Εκδόσεις Νομική Βιβλιοθήκη, 2006

Ανέκδοτες Πηγές (Εργασίες / Διατριβές)

Καρύδα Σπυριδούλα, «ΓΚΠΔ και ν. 4624/2019. Μία ιστορική μεταρρύθμιση του εθνικού νομοθετικού πλαισίου για την προστασία του θεμελιώδους δικαιώματος της προστασίας των δεδομένων προσωπικού χαρακτήρα του ατόμου. Νέες προκλήσεις στη σύγχρονη ψηφιακή εποχή. Διάλογος μεταξύ ενωσιακού και εθνικού νομοθέτη»

Ηλεκτρονικά βιβλία (e-books)

Μαυρίδης Ιωάννης, Ασφάλεια Πληροφοριών στο Διαδίκτυο, Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών, 2005

Έντυπα περιοδικά

Αλεξανδροπούλου - Αιγυπτιάδου Ευγενία, Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων), ΔΙΤΕ (π. ΔΙΜΕΕ), Τεύχος 1/2016

Αλεξανδροπούλου - Αιγυπτιάδου Ευγενία, "Νομική Διασφάλιση του απορρήτου των κινητών επικοινωνιών", ΔΙΜΕΕ 5 (Οκτ-Νοε-Δεκ 2008)

Ιγγλεζάκης Δ. Ιωάννης, Ι., Η ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα (EU-US Privacy Shield), Συνήγορος 113/2016

Μήτρου Λίλιαν, Privacy by Design Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔΙΤΕ (π. ΔΙΜΕΕ), τεύχος 1/2013

Παναγοπούλου-Κουτνατζή Φερενίκη, Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση, Μελέτες, Απόψεις, ΕφημΔΔ-1/2017

Παναγοπούλου-Κουτνατζή Φερενίκη, Το δικαίωμα στη λήθη στην εποχή της αβάσταχτης μνήμης: Σκέψεις αναφορικά με την Πρόταση Κανονισμού Προστασίας Δεδομένων, ΕφημΔΔ 2012

Ηλεκτρονικά Περιοδικά

Ιγγλεζάκης Δ. Ιωάννης, Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων, Επιθεώρηση Δικαίου Πληροφορικής, Τομ. 1, τεύχ. 1, 2020

Ιστοσελίδες

Όπλο κατά των επιδημιών τα ανωνυμοποιημένα δεδομένα, Το Βήμα, 2018, https://www.tovima.gr/2018/02/26/society/oplo-kata-twn-epidimiwn-ta-anwnymopoiimena-dedomena/

Βιβλιογραφία στην Αγγλική Γλώσσα

Ηλεκτρονικά βιβλία (e-books)

Antonopoulos A. / Wood G., Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media, Sebastopol, 2019

Avižienis, A., Lapire, J.C., Randell, B. & Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Computer Society, 1(1), 2004

Bambara J. Allen P., Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions, McGraw-Hill Education, 2018

Brooks, R. Introduction to Computer and Network Security—Navigating the Shades of Gray. London: CRC Press, 2014

Camp, J. Trust and Risk in Internet Commerce, Cambridge: MIT Press, 2000

Campbell Dennis and Fisher Joy, Data Transmission and Privacy, Netherlands: Kluwer Academic Publishers/ Martinus Nijhoff Publishers, 1994

Cozzens, M. & Miller, S, The Mathematics of Encryption: An Elementary Introduction. Mathematical World, 29, American Mathematical Society, 2013

Dwork, C. Differential privacy. In Automata, languages and programming, Springer Berlin Heidelberg, 2006

Esayas, S.Y., The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach [Electronic version]. European Journal of Law and Technology, 6(2), 2015

Feiler Lukas, «The EU General Data Protection Regulation (GDPR): A commentary», Globe law and business, 2018

Ferguson, N. & Schneier, B, Practical Cryptography. Indianapolis: Wiley, 2003

Ferguson, N., Schneier, B. & Kohno, T. Cryptography Engineering: Design Principles and Practical Applications. Indianapolis: Wiley, 2010

Garcia F.D., Jacobs B, Privacy-Friendly Energy-Metering via Homomorphic Encryption, Springer, Berlin, Heidelberg, 2011, https://doi.org/10.1007/978-3-642-22444-7_15

Garrett, P, Making, Breaking Codes: An Introduction to Cryptology. New Jersey: Prentice Hall, 2011

Mougayar William, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, Wiley, 2016

Mukhopadhyay M., Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, Packt Publishing, Birmingham, 2018

Neisse Ricardo, Steri Gary, Nai-Fovino Igor, A Blockchain-based Approach for Data Accountability and Provenance Tracking, 2017, https://doi.org/10.1145/3098954.3098958

Raskin Max, The Law And Legality Of Smart Contracts, 2017

Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M, 'On blockchain and its integration with IoT. Challenges and opportunities', Future Generation Computer Systems Elsevier BV, 2018

Rocher Luc, Hendrickx M. Julien & De Montjoye Yves-Alexandre, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications, 2019

Stalla-Bourdillon Sophie, Phillips Joshua, Ryan D. Mark, Privacy vs. Security

Stallings, W, Cryptography and Network Security—Principles and Practice (6th edition). Boston: Pearson, 2014

Stapleton, J.J. Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity. London: CRC Press, 2014

Tamò-Larrieux Aurelia, Designing for Privacy and its Legal Framework, Springer, 2018

Karageorgiou Dr Stavros J. and Billiri, Fotini “Greece” στο Data Protection Laws of the World, London: Sweet & Maxwell, 1998

Wright David, Should Privacy Impact Assessments Be Mandatory?, Communications of the ACM, July 2011

Zoumpoulidis Stavros, Will Blockchain Technology, Smart Contracts & IoT be the new Lifeblood of Commerce?, Επιθεώρηση Δικαίου Πληροφορικής Τόμ. 1, Αρ. 2 (2020)

Ηλεκτρονικά Περιοδικά

Van Lieshout M., Kool L., Van Schoonhoven B. and de Jong M., Privacy by Design: an alternative to existing practice in safeguarding privacy, Research Gate, 2011

Guegan Dominique. Public Blockchain versus Private blockchain, 2017. ffhalshs-01524440

Ιστοσελίδες

Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

Felten, Ed., Protecting privacy by adding noise., 2012, url: https://techatftc.wordpress.com/2012/06/21/protecting-privacy-by-adding-noise/

Netflix: how to check if your account has been hacked - and how to fix it, 2015, url: https://www.independent.co.uk/life-style/gadgets-and-tech/news/netflix-hacked-recently-watched-fix-a6759336.htm

Swanson T. ‘Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems’, 2015, https://www.ofnumbers.com/2015/04/06/consensus-as-a-service-a-brief-report-on-the-emergence-of-permissioned-distributedledger-systems

Συνέδρια

International Conference of Data Protection and Privacy Commissioners, Privacy by Design Resolution, Jerusalem 2010