ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΑΙ ΟΡΓΑΝΙΣΜΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΟΠΙΚΗ ΑΥΤΟΔΙΟΙΚΗΣΗ

«Ανάπτυξη στρατηγικών ψηφιακής διακυβέρνησης. Μελέτη της περίπτωσης του GDPR»

Παρασκευή Κώτσια

Μεταπτυχιακή Διπλωματική Εργασία

Καλαμάτα, Φεβρουάριος 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΑΙ ΟΡΓΑΝΙΣΜΩΝ

ΚΑΤΕΥΘΥΝΣΗ ΔΙΟΙΚΗΣΗΣ ΟΡΓΑΝΙΣΜΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΟΠΙΚΗ ΑΥΤΟΔΙΟΙΚΗΣΗ

«Ανάπτυξη στρατηγικών ψηφιακής διακυβέρνησης. Μελέτη της περίπτωσης του GDPR.»

Παρασκευή Κώτσια

Μεταπτυχιακή Διπλωματική Εργασία

Επιβλέπων Δρ. Θεόδωρος Κοτσιλιέρης

Εγκρίθηκε από την τριμελή επιτροπή αξιολόγησης 11/03/2022

κ. Θεόδωρος Κοτσιλιέρης

κ. Γεωργόπουλος Ευστράτιος

κα Αναστασία Βουτυνιώτη

Καλαμάτα, Φεβρουάριος 2022

UNIVERISITY OF PELOPPONESE

DEPARTMENT OF BUSINESS ADMINISTRATION AND ORGANIZATIONS

POSTGRADUATE PROGRAM MSc-MPA: PUBLIC ADMINISTRATION and LOCAL GOVERNMENT

"Development of digital governance strategies. The GDPR case study."

Kotsia Paraskevi

Kalamata, February 2022

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω το Πανεπιστήμιο Πελοποννήσου που μου πρόσφερε την ευκαιρία να παρακολουθήσω το Μεταπτυχιακό Πρόγραμμα της Σχολής Δημόσιας Διοίκησης και Τοπικής Αυτοδιοίκησης, που θα συνεισφέρει στην επαγγελματική μου σταδιοδρομία και ιδιαίτερα τον καθηγητή μου κ. Κοτσιλιέρη Θεόδωρο για τη βοήθεια και την καθοδήγησή του με τις κατάλληλες επιστημονικές πρακτικές και άμεσες συμβουλές επί της οργάνωσης και της δομής της παρούσας εργασίας.

Ευχαριστώ θερμά την οικογένειά μου για την υπομονή, τη στήριξη και τη συμπαράσταση που μου προσφέρει σε κάθε μου βήμα, δίνοντάς μου ελπίδα και δύναμη να συνεχίσω για το καλύτερο. Τέλος, ευχαριστώ επίσης τους συναδέλφους και φίλους του μεταπτυχιακού προγράμματος για την αλληλοσυμπαράσταση και υποστήριξη καθ’ όλη τη διάρκεια της κοινής μας εκπαιδευτικής εμπειρίας.

ΑΦΙΕΡΩΣΗ

Στην Ελένη και στον Γρηγόρη…..

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία παρουσιάζει την ψηφιακή διακυβέρνηση με τις κατευθυντήριες αρχές της και τον ψηφιακό μετασχηματισμό με τους κεντρικούς άξονες παρέμβασης, που υλοποιούνται μέσα από την υιοθέτηση των αρχών της ψηφιακής διακυβέρνησης.

Γίνεται παρουσίαση του Γενικού Κανονισμού για την Προστασία των Δεδομένων ΓΚΠΔ/GDPR, με αρχή της εφαρμογής του την 25η Μαΐου 2018, και αναλύεται τι είναι τα προσωπικά δεδομένα, η επεξεργασία τους, οι αρχές προστασίας δεδομένων, η ασφάλεια και τα μέτρα που λαμβάνονται για την προστασία των πληροφοριών.

Στο τρίτο και τέταρτο κεφάλαιο γίνεται εκτενέστερη αναφορά στην εφαρμογή του GDPR σε διάφορους τομείς, όπως η Υγεία, η πανδημία του Covid-19, οι επιχειρήσεις και η Ψηφιακή Διακυβέρνηση. Στο πέμπτο γίνεται αναφορά κυρίως σε περιπτώσεις διαρροής προσωπικών δεδομένων, όπου έχουν επιβληθεί υψηλά πρόστιμα από την Αρχή Προστασίας των Δεδομένων.

Στο τελευταίο κεφάλαιο αναλύεται ο τρόπος με τον οποίον ο GDPR θα αλλάξει τον κόσμο και παρουσιάζονται τα συμπεράσματα από σχετική συνέντευξη με υπεύθυνο του Πανεπιστημίου Πελοποννήσου.

Για τη συνολική συγγραφή της διπλωματικής εργασίας κρίθηκε σκόπιμο η προσέγγιση του θέματος να γίνει με βιβλιογραφική μελέτη και με διεξαγωγή συνέντευξης.

Λέξεις – κλειδιά: Ψηφιακή Διακυβέρνηση, Γενικός Κανονισμός προστασίας δεδομένων, προσωπικά δεδομένα, συμμόρφωση, ασφάλεια.

ABSTRACT

This paper presents digital governance with its guiding principles and digital transformation with the central axes of intervention, which are implemented through the adoption of the principles of digital governance.

The General Regulation for the Protection of Data GPD / GDPR is presented, starting from its implementation on May 25, 2018, and analyzes what is personal data, their processing, data protection principles and security and information measures.

The third and fourth chapters provide a more detailed account of the implementation of the GDPR in various areas, such as Health, the Covid-19 pandemic, business and Digital Governance. The fifth refers mainly to cases of personal data leakage, where high fines have been imposed by the Data Protection Authority.

The last chapter analyzes the way in which the GDPR will change the world and presents the conclusions from a relevant interview with the head of the University of Peloponnese.

Keywords: Digital Governance, General Data Protection Regulation, personal data, compliance, security.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη των Τεχνολογιών Πληροφορίας και Επικοινωνίας (ΤΠΕ) επηρεάζει όλους τους τομείς παγκοσμίως. Οι μεταβολές που συντελούνται σε όλα τα επίπεδα είναι σαφές πως «καλούν» τις κυβερνήσεις των κρατών να αντιμετωπίσουν μια σειρά από προκλήσεις, που σχετίζονται άμεσα με την εισαγωγή των τεχνολογικών εφαρμογών και με την ψηφιοποίηση των διαδικασιών σε όλες τις δράσεις της καθημερινότητας των πολιτών και επιχειρήσεων (Παρασκευάς Μ., Ασημακόπουλος Γ., Τριανταφύλλου Β., 2017)

Η ταχύτητα με την οποία αναπτύσσεται η ψηφιακή διακυβέρνηση είναι ενδεικτική της ανάγκης να κατέχει κεντρικό ρόλο, ώστε τα κράτη να καταφέρουν να αντιμετωπίσουν αυτές τις προκλήσεις μέσα από τη χρήση μιας σειράς από αναδυόμενες ψηφιακές ευκαιρίες (Virkar S., Edelmann N., Hynek N., Parycek P., 2019). Ο ψηφιακός μετασχηματισμός της Δημόσιας Διοίκησης καθίσταται στρατηγική προτεραιότητα των κυβερνήσεων παγκοσμίως, καθώς η Ψηφιακή Διακυβέρνηση βελτιώνει την αποτελεσματικότητα και την ποιότητα των Δημόσιων Υπηρεσιών και δημιουργεί νέο περιβάλλον αλληλεπίδρασης και επικοινωνίας των πολιτών με τη Δημόσια Διοίκηση και τις κυβερνήσεις.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ/GDPR) αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ανεξέλεγκτης κυκλοφορίας των δεδομένων αυτών και πρόκειται να αντικαταστήσει την Οδηγία του Ευρωπαϊκού Κοινοβουλίου 95/46/ΕΚ (24/10/1995) «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Η ψήφιση του ΓΚΠΔ/GDPR έγινε στις 27 Απριλίου 2016 και η εφαρμογή του άρχισε στις 25

Μαΐου 2018. Οι επιχειρήσεις - οργανισμοί θα πρέπει να συμμορφωθούν ως προς την εφαρμογή του κανονισμού.

Η ανάπτυξη της τεχνολογίας και των κοινωνικών μέσων δικτύωσης έχει αλλάξει σε μεγάλο βαθμό τις ζωές μας. Σήμερα, τα προσωπικά μας δεδομένα είναι εκτεθειμένα περισσότερο από ποτέ, ενώ ο κίνδυνος της αυθαίρετης έως κακόβουλης επεξεργασίας και χρήσης τους καθιστά επιτακτική την ανάγκη προστασίας τους. Η εφαρμογή του ΓΚΠΔ/GDPR σε διάφορους τομείς, όπως στην Υγεία, στην πανδημία του COVID-19, στις επιχειρήσεις και στην ψηφιακή διακυβέρνηση, καθίσταται απολύτως αναγκαία.

ΚΕΦΑΛΑΙΟ 1: ΨΗΦΙΑΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ

Η Ψηφιακή Διακυβέρνηση στοχεύει στην ανάπτυξη και στην εξάπλωση των Τεχνολογιών Πληροφορικής και Επικοινωνίας χρησιμοποιώντας τις κατάλληλες τεχνολογίες σε όλα τα επίπεδα υποδομών, τις κατάλληλες γνώσεις και δεξιότητες και την επιθυμία για αναπτυξιακές μεταβολές.

1.1 ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΑΡΧΕΣ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Αναφορικά με τον ψηφιακό μετασχηματισμό του δημόσιου φορέα, ορίζονται ένα πλήθος κατευθυντήριων γραμμών, ο πυρήνας των οποίων στηρίζεται στην ψηφιακή διακυβέρνηση. Αυτές έχουν αποτυπωθεί μέσα από πρωτοβουλίες που αναλήφθηκαν από την Ευρωπαϊκή Ένωση και από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης στο Ταλίν της Εσθονίας το 2017. Εκεί υπογράφηκε από όλα τα κράτη – μέλη της Ευρωπαϊκής Ένωσης (28 στον αριθμό) η ομώνυμη Διακήρυξη, αποτελώντας τη συνέχεια του Σχεδίου Δράσης για την Ηλεκτρονική Διακυβέρνηση (2016 – 2020), καθώς και του Ευρωπαϊκού Πλαισίου Διαλειτουργικότητας (ec.europa.eu., 2017).

Μέσα από τη Διακήρυξη αυτή δίνεται ιδιαίτερη έμφαση σε έναν σχεδιασμό με επίκεντρο τον πολίτη, παρέχοντας παράλληλα ψηφιακές, αλλά και διασυνοριακές υπηρεσίες προς το σύνολο των επιχειρηματικών οντοτήτων της Κοινότητας. Συνοπτικά, οι κατευθυντήριες αρχές της Ψηφιακής Διακυβέρνησης, όπως αυτές περιγράφονται στη Διακήρυξη του Ταλίν, είναι βασικός παράγοντας για την επίτευξη ενός ψηφιακού μετασχηματισμού (Υπουργείο Εσωτερικών, 2020).

Μέσα από την παροχή ψηφιακών υπηρεσιών επιδιώκεται αρχικά η μείωση της διακίνησης εγγράφων σε φυσική μορφή και παράλληλα η προώθηση της χρήσης ψηφιακών δεδομένων ανάμεσα στους διαφόρους φορείς του

δημόσιου τομέα, με στόχο την εξυπηρέτηση πολιτών αλλά και επιχειρήσεων (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Σε μια τέτοια περίπτωση, ο ενδιαφερόμενος δεν θα προβαίνει στη φυσική κατάθεση δικαιολογητικών σε μια υπηρεσία, αλλά αντίθετα, τα έγγραφα αυτά θα παράγονται και θα διατίθενται με ηλεκτρονικό τρόπο. Μέσα στα πλαίσια της αρχής αυτής είναι και η προαγωγή δράσεων που θα άπτονται της συνεχούς βελτίωσης αλλά και της ανάπτυξης μιας νοοτροπίας από τους πολίτες και τις επιχειρήσεις, προκειμένου να διαθέτουν τις κατάλληλες εκείνες δεξιότητες για την πλήρη και αποτελεσματική χρήση των Τεχνολογιών Πληροφορίας και Επικοινωνίας.

Σύμφωνα με την αρχή αυτή, οι πολίτες και οι επιχειρήσεις θα πρέπει να υποβάλουν μόνο μια φορά, όλες εκείνες τις απαιτούμενες πληροφορίες και στοιχεία που άπτονται της αλληλεπίδρασής τους με τις Δημόσιες Αρχές (Υπουργείο Εσωτερικών, 2020). Με τον τρόπο αυτό απαλλάσσονται από την ανάγκη να παρέχουν σε κάθε τους συναλλαγή το σύνολο των εντύπων και των πληροφοριών, που σε μεγάλο βαθμό είναι ήδη γνωστές στους κρατικούς φορείς, μειώνοντας το κόστος και τον χρόνο μιας συναλλαγής. Αυτό που απαιτείται σε αυτή την περίπτωση είναι μόνο η πλήρης προστασία των προσωπικών δεδομένων πολιτών και επιχειρήσεων από τους δημόσιους φορείς, μιας και θα υπάρχει διαμοιρασμός αυτών των πληροφοριών μεταξύ τους και κατά συνέπεια θα πρέπει να λαμβάνονται τα κατάλληλα μέτρα.

Με στόχο τον σχεδιασμό μιας σειράς από αλληλένδετες και με επίκεντρο τους πολίτες και τις υπηρεσίες πολιτικών, χρειάζεται η υιοθέτηση εκείνων που θα διέπονται από διαλειτουργικότητα. Με τον τρόπο αυτό θα εξασφαλίζεται η αδιάλειπτη λειτουργία των εργασιών, ενώ παράλληλα καταργούνται και μια σειρά από «στεγανά», που εμποδίζουν την

αμεσότητα ως προς την παροχή υπηρεσιών προς τους ενδιαφερόμενους (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Η ανάπτυξη της τεχνολογίας και των εφαρμογών της οδηγεί στην αναγκαιότητα για την παροχή ψηφιακών υπηρεσιών κατά προτεραιότητα μέσω της χρήσης «έξυπνων» κινητών συσκευών. Θα πρέπει να παρέχεται προς τους χρήστες των κινητών αυτών συσκευών η δυνατότητα πρόσβασης στις ηλεκτρονικές υπηρεσίες ανεξάρτητα από τον τύπο αυτής της συσκευής, ενώ, παράλληλα, για την προαγωγή της λύσης αυτής θα πρέπει η εξυπηρέτηση των πολιτών να γίνεται κατά προτεραιότητα με την εξής σειρά: μέσω των κινητών τηλεφώνων, των ηλεκτρονικών υπολογιστών, της τηλεφωνικής εξυπηρέτησης, των ταχυδρομικών επιστολών και της φυσικής παρουσίας στους δημόσιους φορείς.

Οι ψηφιακές υπηρεσίες, που θα σχεδιασθούν, απαιτείται να έχουν ως επίκεντρό τους τον πολίτη και την παροχή όσο το δυνατόν περισσότερο ολοκληρωμένων αλλά και στοχευμένων στην κάλυψη των αναγκών του υπηρεσιών. Έτσι, οι πολίτες και οι επιχειρήσεις θα μπορούν να επιλέγουν τη συναλλαγή με τους δημόσιους φορείς με τρόπους ψηφιακούς, μέσα από ένα πλήθος υπηρεσιών που παρουσιάζουν αυξημένη προσβασιμότητα, διαθεσιμότητα, καθώς και ασφάλεια και ευχρηστία (Υπουργείο Εσωτερικών, 2020).

Για να αξιοποιηθούν σωστά οι ψηφιακές υπηρεσίες θα πρέπει να υπάρχουν σύγχρονα μοντέλα ανάπτυξης, μέσα από τα οποία θα εξασφαλίζεται η εκ νέου χρήση των δομικών εκείνων στοιχείων και λύσεων, ενώ παράλληλα θα υιοθετούν κάποια διαδεδομένα πρότυπα και θα τηρούν συγκεκριμένες προδιαγραφές ποιότητας. Προς την κατεύθυνση αυτή απαιτείται η προώθηση μιας σειράς από λύσεις και πρότυπα τα οποία θα στηρίζονται στη διαλειτουργικότητα, στη μείωση της γραφειοκρατίας και γενικότερα

στην ενίσχυση της ηλεκτρονικής διακυβέρνησης (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Ανοικτές και συμμετοχικές διαδικασίες και σχεδιασμός ψηφιακών υπηρεσιών

Τηρώντας μια σειρά από συνεργατικές διαδικασίες συνδιαμόρφωσης με το σύνολο των εμπλεκόμενων μερών, καθίσταται εφικτή η εκτίμηση των υφιστάμενων ψηφιακών υπηρεσιών, αλλά και ο υπολογισμός κάθε καινούργιας και πιο απλουστευμένης. Στόχος θα πρέπει να είναι ο κατάλληλος σχεδιασμός εκείνων των ψηφιακών δημόσιων υπηρεσιών, οι οποίες και θα ανταποκρίνονται στις απαιτήσεις και τις ανάγκες πολιτών και επιχειρήσεων.

Καθολική προσβασιμότητα και κατάργηση των αποκλεισμών

Στο σύνολο των ψηφιακών υπηρεσιών θα έχει πρόσβαση ο κάθε ενδιαφερόμενος και όχι μόνο όσοι εμφανίζουν υψηλό επίπεδο ψηφιακής εξοικείωσης. Απαιτείται κατάργηση των όποιων περιορισμών υπάρχουν για άτομα είτε με αναπηρίες, είτε που ανήκουν σε ευπαθείς ομάδες, είτε ακόμη και για όσους έχουν μεγαλύτερη ηλικία (Υπουργείο Εσωτερικών, 2020).

Διασυνοριακή εξυπηρέτηση πολιτών

Μέσα από τον ψηφιακό μετασχηματισμό απαιτείται η διευκόλυνση της εξυπηρέτησης των πολιτών που ανήκουν στα κράτη – μέλη της Ευρωπαϊκής Ένωσης με συνέπεια την ελεύθερη μετακίνηση δεδομένων. Επομένως, οι αρμόδιες αρχές απαιτείται να προβούν στην άμεση διαθεσιμότητα του συνόλου των ψηφιακών υπηρεσιών, αποβλέποντας στην απρόσκοπτη λειτουργία, αλλά και στην ελεύθερη μετακίνηση των δεδομένων, ώστε να αξιοποιούνται με τρόπο άμεσο και αποτελεσματικό.

Αξιοπιστία – εμπιστοσύνη

Η αξιοπιστία και η εμπιστοσύνη από τους πολίτες και τις επιχειρήσεις προς τις ψηφιακές υπηρεσίες εξασφαλίζεται μέσα από την ευχρηστία τους, αλλά και μέσα από τη συνεχή και αδιάλειπτη διαθεσιμότητά τους. Το νομοθετικό πλαίσιο λειτουργίας αυτών των υπηρεσιών προϋποθέτει την εγγύηση της προστασίας δεδομένων προσωπικού χαρακτήρα αλλά και της ιδιωτικής ζωής των πολιτών.

Ενίσχυση διαφάνειας

Ο διαμοιρασμός των δεδομένων των πολιτών και των επιχειρήσεων μεταξύ των δημόσιων φορέων προϋποθέτει από την πλευρά των φορέων την εξασφάλιση ελέγχου ως προς την πρόσβασή τους σε δεδομένα και τυχόν διόρθωση αυτών στις περιπτώσεις αλλαγής τους. Παράλληλα, πολίτες και επιχειρήσεις θα πρέπει να παρακολουθούν τον σχεδιασμό και την παροχή υπηρεσιών, ώστε με τον τρόπο αυτό να αυξάνεται η διαφάνεια, σε σχέση με τον τρόπο λειτουργίας της Δημόσιας Διοίκησης, εξασφαλίζοντας έτσι και την ενημέρωσή τους (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

Ανάπτυξη ασφαλούς λογισμικού και συστημάτων

Η υιοθέτηση και κυρίως η συνεχής και αδιάλειπτη χρήση των ψηφιακών υπηρεσιών από τους πολίτες και τις επιχειρήσεις προϋποθέτει την ύπαρξη συστημάτων υψηλής ασφάλειας, που παρέχονται από τους ίδιους τους φορείς του Δημοσίου. Μέσα σε αυτό το πλαίσιο επομένως θα πρέπει να ενσωματώνονται κατά τον σχεδιασμό τους τα κατάλληλα πρότυπα ανάπτυξης ασφαλούς λογισμικού και συστημάτων, με συνεχή ενημέρωση ως προς τα διαθέσιμα εργαλεία και τους μηχανισμούς, που μπορούν να χρησιμοποιηθούν.

<u>Απλοποίηση διαδικασιών</u>

Τέλος, μια ακόμη αρχή είναι και αυτή της απλοποίησης των διαδικασιών σχετικά με τις δράσεις που οριοθετούνται και που υλοποιούνται. Αυτές δεν θα πρέπει να είναι διασκορπισμένες και μεμονωμένες, αλλά να διακρίνονται από συντονισμό και κυρίως απλότητα στη χρήση και στην κατανόησή τους (Υπουργείο Εσωτερικών, 2020).

1.1.1 ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

Σε μεγάλο βαθμό τόσο η ανάπτυξη της εθνικής οικονομίας μιας χώρας, όσο και γενικότερα η κοινωνική της ευημερία επηρεάζεται πλέον από τον βαθμό στον οποίο επιτυγχάνεται με αποτελεσματικότητα ο ψηφιακός της μετασχηματισμός. Η έννοια του μετασχηματισμού αναφέρεται στη μετατροπή μιας υφιστάμενης διαδικασίας από χειρωνακτική σε ψηφιακή, μέσα από την τήρηση μιας σειράς σταδιακών και σταθερών βημάτων. Απαιτείται έμφαση στις ψηφιακές δεξιότητες των ατόμων και παράλληλα, η υποστήριξη της επιχειρηματικότητας, μέσα από τη βελτίωση και ενδυνάμωση των υποδομών, διαμορφώνοντας ένα πλήρες και λειτουργικό ψηφιακό κράτος (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020). Τίθενται όμως μια σειρά από ερωτήματα, αναφορικά με την έννοια και το περιεχόμενο του ψηφιακού μετασχηματισμού.

Αρχικά, με την έννοια ψηφιακός μετασχηματισμός γίνεται αναφορά στη δημιουργία των ψηφιακών οδών ολοκλήρωσης των διαδικασιών που εφαρμόζονται καθημερινά στην παραγωγική διαδικασία, αλλά και στις παρεχόμενες υπηρεσίες, που ένας οργανισμός μπορεί να διαθέτει (Virkar S., Edelmann N., Hynek N., Parycek P., 2019). Καλείται ψηφιακός διότι απαιτείται η χρήση διαφόρων ηλεκτρονικών μέσων, που μπορεί να είναι έξυπνα κινητά τηλέφωνα ή εφαρμογές σε ηλεκτρονικούς υπολογιστές, καθώς και ρομποτικές εφαρμογές, σε αντικατάσταση χειρωνακτικών

εργασιών, που επιτελούνταν έως εκείνη τη στιγμή (Virkar S., Edelmann N., Hynek N., Parycek P., 2019). Αυτές οι εργασίες και οι διαδικασίες μπορεί να έχουν εσωτερικό ή εξωτερικό χαρακτήρα. Οι πρώτες, οι εσωτερικές, αφορούν τις διαδικασίες που χρησιμοποιούνται για τη συνεργασία ανάμεσα σε τμήματα ή φορείς, ενώ οι δεύτερες, οι εξωτερικές, σχετίζονται με παροχή προϊόντων και υπηρεσιών, στις οποίες υπάρχει άμεση ή έμμεση εμπλοκή τρίτων, (δηλ. άτομα και επιχειρήσεις).

Ο ψηφιακός μετασχηματισμός στη Δημόσια Διοίκηση έχει ως στόχο τον καταμερισμό του συνόλου των αρμοδιοτήτων, οι οποίες σε πολλές περιπτώσεις περιλαμβάνουν αποσπασματικές και επικαλυπτόμενες δράσεις, που ασκούνται από διαφορετικούς οργανισμούς και φορείς (Mergel I., Kattel R., Lember V., Mcbride K., 2018).

Μέσα από τον ψηφιακό μετασχηματισμό επιδιώκεται η αντιμετώπιση τόσο της απουσίας συντονισμού, όσο και της μη σωστής ιεράρχησης των αρμοδιοτήτων και προτεραιοτήτων, η οποία οδηγεί σε ένα έλλειμμα στόχευσης και σε ένα μη επιθυμητό αποτέλεσμα. Βασικό συστατικό στοιχείο του ψηφιακού μετασχηματισμού είναι η ύπαρξη ενός ενιαίου και παράλληλα δεσμευτικού μοντέλου άσκησης διοίκησης από την πλευρά του κράτους, μέσα στο οποίο θα εμπεριέχονται οι φορείς της κυβέρνησης, αλλά και οι φορείς του δημόσιου τομέα.

Επίσης, αυτό το «νέο μοντέλο», θα προσδιορίσει τους ρόλους και τις αρμοδιότητες των φορέων της Δημόσιας Διοίκησης. Ο σκοπός μιας τέτοιας διαδικασίας είναι η εξασφάλιση, με τη συνδρομή και τη συνεργασία του ιδιωτικού τομέα, ενός περιβάλλοντος διαφάνειας, αποδοτικότητας και αποτελεσματικότητας, το οποίο θα έχει ξεκάθαρους ρόλους για τον κάθε φορέα και τις αρμοδιότητές του. Η ανάπτυξη του ψηφιακού μετασχηματισμού, που συντελείται τα τελευταία έτη παγκοσμίως και η

οποία αναμένεται να ενταθεί, βασίζεται σε τέσσερις αλληλοσυμπληρούμενες και αλληλοενισχυόμενες δυνάμεις. Αυτές είναι σύμφωνα με τον Σύνδεσμο Επιχειρήσεων και Βιομηχανιών (2019):

- ***Η ανάπτυξη της τεχνολογίας***

Οι πιο βασικές τεχνολογίες, που αφορούν στην υπολογιστική ισχύ, στην αποθήκευση και στη μετάδοση των δεδομένων, παρουσιάζουν εκθετική ανάπτυξη, με υψηλή επίσης, από την άλλη πλευρά, μείωση του κόστους. Κατά συνέπεια, μέσα από αυτήν τη διαδικασία υπάρχει η επίτευξη ισχυρών τεχνολογικών επιτευγμάτων, τα οποία μελλοντικά θα ενισχυθούν ακόμη περισσότερο.

- ***Η συνδυαστική καινοτομία***

Η φύση των ψηφιακών τεχνολογιών, επιτρέπει την ύπαρξη ενός συνδυασμού ανάμεσά τους, με στόχο την παραγωγή συνεχώς νέων καινοτομιών. Μέσα από την εκάστοτε τεχνολογία, μπορεί να αυξηθεί και ο πιθανός αριθμός των δυνατών συνδυασμών, ενώ παράλληλα τα αποτελέσματα, που επιτυγχάνονται αποκτούν νέες μορφές και σημαντική δυναμική.

- ***Η ροή διασποράς***

Οι ψηφιακές τεχνολογίες μπορούν να φτάνουν σε μεγάλη κλίμακα και να διασπείρονται άμεσα στην περίπτωση κατά την οποία τα προσφερόμενα αποτελέσματα ικανοποιούν τις πραγματικές ανάγκες των ενδιαφερόμενων.

- ***Οι ανατέλλουσες τεχνολογίες***

Οι ψηφιακές τεχνολογίες αποτελούν ένα ετερογενές σύνολο και εντοπίζονται σε διαφορετικές φάσεις ωριμότητας. Ορισμένες από αυτές θεωρείται πως θα προκαλέσουν τις πιο σημαντικές αλλαγές και

τοποθετούνται ακόμη σε αρχικά στάδια, χωρίς όμως να υπάρχει ξεκάθαρη εικόνα σχετικά με το τι πρόκειται να συμβεί μελλοντικά.

1.1.2 ΟΙ ΕΠΕΡΧΟΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Οι ψηφιακές τεχνολογίες θεωρούνται πως θα προκαλέσουν σημαντικότερες αλλαγές και θεωρείται πως βρίσκονται ακόμη σε πρώιμο στάδιο, χωρίς όμως να υπάρχει ξεκάθαρη εικόνα σχετικά με το τι πρόκειται να συμβεί μελλοντικά. Τέλος, αναφορικά με τα οφέλη που προκύπτουν μέσα από τον ψηφιακό μετασχηματισμό, αυτά συνοψίζονται (Σύνδεσμος Επιχειρήσεων και Βιομηχανιών, 2019):

i. Στην αναβάθμιση της εξυπηρέτησης προς τους πολίτες και τις επιχειρήσεις από τους δημόσιους φορείς, μιας και υπάρχει η δυνατότητα της πρόσβασης κάθε στιγμή εντός της ημέρας σε οποιαδήποτε υπηρεσία, εκμηδενίζοντας τόσο τον χρόνο της μετακίνησης, όσο και τον χρόνο της αναμονής, εξασφαλίζοντας παράλληλα και υψηλό επίπεδο διαφάνειας.

ii. Στα οφέλη που αποκομίζει το ίδιο το κράτος: μέσα από τη χρήση ψηφιακών εργαλείων οι δημόσιοι φορείς μπορούν να «αυτοεξυπηρετηθούν» καταναλώνοντας λιγότερους πόρους, μειώνοντας τη γραφειοκρατία και κυρίως επιτυγχάνοντας πιο ποιοτικό αποτέλεσμα.

iii. Όταν οι ψηφιακές υπηρεσίες είναι κατάλληλα σχεδιασμένες για την εκπλήρωση των αναγκών των πολιτών και των επιχειρήσεων, τότε παρέχονται σημαντικά κίνητρα προς τους ενδιαφερόμενους για να τις χρησιμοποιήσουν. Επομένως μέσα από έναν τέτοιο σχεδιασμό, καθίσταται σαφές πως ικανοποιείται ο στόχος του κράτους και οι πολίτες – επιχειρήσεις απολαμβάνουν υψηλού επιπέδου υπηρεσίες.

1.2 ΑΞΟΝΕΣ ΠΑΡΕΜΒΑΣΗΣ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Οι βασικοί στρατηγικοί άξονες παρέμβασης της ψηφιακής διακυβέρνησης, επικεντρώνονται στα εξής:

- ***Συνδεσιμότητα***

Στη νέα ψηφιακή εποχή η συνδεσιμότητα είναι η πιο βασική απαίτηση για τον ψηφιακό μετασχηματισμό των κρατών. Εάν τα κράτη διασφαλίσουν την ευρεία εγκατάσταση δικτύων και την παροχή των υπηρεσιών τους για πολύ υψηλή χωρητικότητα σε όλη την επικράτειά τους, θα επιτύχουν πολλά θετικά σε επίπεδο κοινωνίας και οικονομίας. Η συνδεσιμότητα επικεντρώνεται στην επίτευξη των κάτωθι στόχων (Πομπόρτσης Α., 2017):

i. Διασφάλιση εξαιρετικά υψηλών ταχυτήτων στο σύνολο των κεντρικών οικονομικών αλλά και κοινωνικών μοχλών ενός κράτους, όπως είναι οι φορείς του Δημοσίου, τα ερευνητικά κέντρα, τα εκπαιδευτικά ιδρύματα, αλλά και τα νοσοκομεία και οι μεταφορές.

ii. Αδιάλειπτη κάλυψη υψηλών ταχυτήτων στους ανωτέρω κεντρικούς οικονομικούς και κοινωνικούς μοχλούς του κράτους

iii. Παροχή πρόσβασης στο σύνολο των πολιτών και των επιχειρήσεων, σε όποια περιοχή και εάν βρίσκονται, είτε εντός είτε εκτός αστικού ιστού.

- ***Ψηφιακές Ικανότητες και δεξιότητες***

Η τεχνολογική επανάσταση που συντελείται απαιτεί την ισχυρή και πλήρη, σε όλα τα επίπεδα, σύμπραξη των ατόμων. Στόχος τους να προλαβαίνουν τη ραγδαία εξέλιξη των μηχανημάτων και να θέτουν γρήγορα το πλαίσιο των ηθικών αξιών και των κανόνων, που θα διασφαλίσουν την ανθρώπινη αξιοπρέπεια και θα διαφυλάξουν τους δημοκρατικούς θεσμούς της χώρας (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020). Η επένδυση στους πολίτες

αποτελεί τον πυρήνα του ψηφιακού μετασχηματισμού μιας χώρας και έτσι, η θέληση για γνώση και η ανάπτυξη των ψηφιακών δεξιοτήτων θα αποτελέσουν την κινητήρια δύναμη με την οποία οι πολίτες μπορούν να παίξουν ενεργό ρόλο και να διαμορφώσουν μαζί με τους κρατικούς φορείς, το πλαίσιο υιοθέτησης και πρόκλησης αλλαγών, ώστε η χώρα τους να επιβιώσει στον παγκόσμιο ανταγωνισμό.

Η ολοκλήρωση του σχεδίου ανάπτυξης στο σύνολο των ψηφιακών δεξιοτήτων επιδιώκει τη σύνδεση σε ένα περιβάλλον όπου οι πολίτες θα νιώθουν εμπιστοσύνη, ασφάλεια και θα είναι ενεργοί, ενώ το κράτος και οι υπηρεσίες θα είναι αποτελεσματικές ως προς την εξυπηρέτηση του πολίτη. Παράλληλα, η οικονομία και η ανάπτυξη μιας χώρας θα είναι προσαρμοσμένες στο ψηφιακό μέλλον και στον διεθνή ανταγωνισμό. Απαιτείται η αξιοποίηση του υφιστάμενου ανθρώπινου κεφαλαίου, που μια χώρα διαθέτει, και η ένωση των δυνάμεων με συνεργασία του δημόσιου και του ιδιωτικού τομέα, σε ακαδημαϊκά ιδρύματα και ερευνητικούς φορείς, σε επιμελητήρια και επαγγελματικές ενώσεις, σε κοινωφελείς οργανισμούς και κοινωνικούς εταίρους (Πομπόρτσης Α., 2017).

Με τις ψηφιακές τεχνολογίες να αλλάζουν την οικονομία, αξιοποιώντας τις ψηφιακές δεξιότητες, ενισχύοντας τα ηλεκτρονικά συστήματα και τις υπηρεσίες μπορούν να ενισχυθούν οι επιχειρησιακές διαδικασίες για την προώθηση εξαγωγών και εισαγωγών της χώρας (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

- ***<u>Ψηφιακές Δημόσιες Υπηρεσίες</u>***

Η ψηφιακή Δημόσια Διοίκηση παρέχει πλέον «έξυπνες» υπηρεσίες προσβάσιμες και διαθέσιμες προς τους πολίτες. Ωστόσο, η γραφειοκρατία δημιουργεί ακόμα διοικητικά προβλήματα και κόστος για τις επιχειρήσεις. Παρά τη γρήγορη πρόοδο όσον αφορά την απλούστευση και την

ψηφιοποίηση των διαδικασιών του Δημοσίου, εκκρεμούν σημαντικά περιθώρια βελτίωσης (Πομπόρτσης Α., 2017).

Οι χρήστες των ψηφιακών υπηρεσιών θα πρέπει να έχουν πρόσβαση στην πληροφορία και στις υπηρεσίες που χρειάζονται. Στη εποχή μας, όλες οι υπηρεσίες παρέχονται από διακριτές σελίδες των φορέων. Όμως, πολλές υπηρεσίες που παρέχονται είναι άγνωστες ακόμα στο ευρύ κοινό. Οι παρεχόμενες υπηρεσίες έχουν τη δική τους φιλοσοφία, εμφάνιση και λειτουργικότητα και έτσι δεν μπορούν να διασφαλίσουν την επικοινωνία που απαιτείται ανάμεσα στον πολίτη και την επιχείρηση με τη Δημόσια Διοίκηση (Υπουργείο Ψηφιακής Διακυβέρνησης, 2020).

- ***Ψηφιακή Καινοτομία***

Η ψηφιακή καινοτομία περιλαμβάνει έργα υποδομής και έργα που αποσκοπούν στην εξυπηρέτηση των επιχειρήσεων και των πολιτών. Τα θετικά αυτής της καινοτομίας είναι η ραγδαία αύξηση της παραγωγικότητας, η μείωση του κόστους παροχής των υπηρεσιών, οι νέες θέσεις εργασίας, η πρόσβαση σε νέες αγορές και άλλα, τα οποία είναι γνωστά για την οικονομική ανάπτυξη μιας χώρας. Ωστόσο, τα οφέλη δεν μπορούν να θεωρηθούν αυτονόητα, γιατί πολλές επιχειρήσεις δυσκολεύονται στην υιοθέτηση νέων τεχνολογιών. Αυτό συμβαίνει διότι η ψηφιακή καινοτομία χρειάζεται την αλλαγή της ψηφιακής κουλτούρας με προϋποθέσεις τα ρυθμιστικά, χρηματοδοτικά και υποστηρικτικά περιβάλλοντα ανάμεσα στο κράτος και την αγορά. Σημαντική προϋπόθεση είναι επίσης η επαρκής σύνδεση και η σύμπραξη των φορέων καινοτομίας (Πομπόρτσης Α., 2017).

ΚΕΦΑΛΑΙΟ 2: ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ (ΓΚΠΔ/GDPR)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού χαρακτήρα (= General Data Privacy Regulation), θεσμοθετήθηκε από την Ευρωπαϊκή Ένωση στις 25 Μαΐου του 2018 με στόχο την προστασία των προσωπικών δεδομένων των πολιτών και τον καθορισμό των τρόπων και των προϋποθέσεων που θα γίνεται η επεξεργασία και η χρήση αυτών των δεδομένων. Προκειμένου να προστατευθούν τα δεδομένα του ατόμου, που συνεργάζεται με μια επιχείρηση ή έναν φορέα (δημόσιο ή ιδιωτικό), ο Κανονισμός υποχρεώνει τις επιχειρήσεις να τηρούν κάποια τεχνικά και οργανωτικά μέτρα.

2.1 ΟΙ ΣΤΟΧΟΙ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Οι στόχοι του Γενικού Κανονισμού της Προστασίας Δεδομένων είναι η προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων και η θέσπιση κανόνων για την προστασία τους, ώστε να επιτραπεί ελεύθερα η κυκλοφορία των δεδομένων εντός της Ε.Ε. Επίσης, ο Γενικός Κανονισμός της Προστασίας Δεδομένων ορίζει αυστηρούς κανόνες για την επεξεργασία των δεδομένων βάσει της συγκατάθεσης. Σκοπός των κανόνων αυτών είναι να διασφαλιστεί ότι το υποκείμενο των δεδομένων κατανοεί για το τι πραγματικά έχει δώσει τη συγκατάθεσή του. Δηλαδή, η συγκατάθεση πρέπει να δίνεται ελεύθερα, συγκεκριμένα και χωρίς ασάφειες με δήλωση διατυπωμένη σε απλή και κατανοητή γλώσσα, για παράδειγμα με μια υπεύθυνη δήλωση. Τέλος, ο Γενικός Κανονισμός Προστασίας των δεδομένων δεν μπορεί να εφαρμοστεί όταν το υποκείμενο των δεδομένων δεν είναι εν ζωή, όταν είναι νομικό πρόσωπο ή η επεξεργασία τους γίνεται από πρόσωπο που ενεργεί για σκοπούς εκτός του εμπορικού, επιχειρηματικού ή επαγγελματικού του πεδίου.

2.2 ΔΕΔΟΜΕΝΑ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Δεδομένα προσωπικού χαρακτήρα είναι τα στοιχεία που ταυτοποιούν ένα πρόσωπο. Μπορεί δηλαδή να είναι ένα ονοματεπώνυμο, ένας Α.Φ.Μ., μια διεύθυνση κατοικίας, ο αριθμός ταυτότητας ή διαβατηρίου, ο κώδικας πρωτοκόλλου διαδικτύου (IP), τα δεδομένα που έχουν οι γιατροί ή τα νοσοκομεία για το κάθε υποκείμενο. Επιπλέον, υπάρχουν τα «Προσωπικά Δεδομένα ειδικής κατηγορίας», η εκμετάλλευση ή η κακόβουλη χρήση των οποίων μπορεί να προσβάλει το υποκείμενο των δεδομένων αυτών σε μεγαλύτερο βαθμό , σε σύγκριση με αυτά της μη ειδικής κατηγορίας, επειδή περιλαμβάνουν ευαίσθητες πληροφορίες για το υποκείμενο.

Ευαίσθητες πληροφορίες, σύμφωνα με το Άρθρο 9 του Κανονισμού 679/2016 Ε.Ε., είναι η αποκάλυψη φυλετικής ή εθνοτικής καταγωγής, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή η συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών ή βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν στην υγεία ή δεδομένων που αφορούν στη σεξουαλική ζωή φυσικού προσώπου ή στον γενετήσιο προσανατολισμό του (Γενικός Κανονισμός Προστασίας Δεδομένων Ε.Ε. 2016/679).

2.2.1 ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Σε μία επιχείρηση δυνατότητα επεξεργασίας των προσωπικών δεδομένων έχει είτε ο υπεύθυνος προστασίας δεδομένων (ΥΠΔ), που μπορεί να έχει οριστεί από την επιχείρηση, είτε ο εκτελών την επεξεργασία, ο οποίος φυλάσσει και επεξεργάζεται τα δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας. Όμως, ο υπεύθυνος προστασίας δεδομένων είναι ο αρμόδιος για την παρακολούθηση της επεξεργασίας των προσωπικών δεδομένων, και οφείλει να ενημερώνει και να συμβουλεύει τους

υπαλλήλους επεξεργασίας προσωπικών δεδομένων σχετικά με τις υποχρεώσεις τους. Επίσης, ο ΥΠΔ συνεργάζεται με την Αρχή Προστασίας Δεδομένων (ΑΠΔ), όποτε κρίνεται απαραίτητο.

Για να επιτραπεί η επεξεργασία των δεδομένων, σύμφωνα με τους κανονισμούς της Ε.Ε., πρέπει αυτή να γίνεται με θεμιτό και νομότυπο τρόπο, για έναν συγκεκριμένο σκοπό και να περιορίζεται στα δεδομένα που είναι αναγκαία για την επίτευξη αυτού του σκοπού. Για την επεξεργασία τους πρέπει να τηρείται ένας από τους παρακάτω όρους: να έχει δοθεί η συγκατάθεση του υποκειμένου των δεδομένων, να τηρείται η συμβατική υποχρέωση έναντι του υποκειμένου των δεδομένων, να υπάρχει η νομική υποχρέωση, να προστατεύονται τα ζωτικά συμφέροντα του υποκειμένου και να εκτελείται ως προς το νόμιμο συμφέρον.

2.2.2 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ GDPR

Με τον Γενικό Κανονισμό 679/2016 Ε.Ε. οφείλουν να συμμορφωθούν όλες οι επιχειρήσεις εντός Ευρωπαϊκής Ένωσης, καθώς και αυτές που, αν και βρίσκονται εκτός Ευρωπαϊκής Ένωσης, πραγματοποιούν συναλλαγές εντός αυτής. Άραγε, τι θα συμβεί αν τα προσωπικά δεδομένα διαρρεύσουν, σε ψηφιακή μορφή στο διαδίκτυο, όπου εκεί δεν υπάρχουν τα περιοριστικά γεωγραφικά πλαίσια; (Γενικός Κανονισμός Προστασίας Δεδομένων Ε.Ε. 2016/679)

2.3 ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Η ασφάλεια των πληροφοριών είναι μία ελεγχόμενη και συνεχής διαδικασία με σκοπό τη διατήρηση και βελτίωση του κατάλληλου επιπέδου ασφαλείας. Η ασφάλεια των πληροφοριών είναι άμεσα συνδεδεμένη με την προστασία των προσωπικών δεδομένων και τον νέο κανονισμό ΓΚΠΔ. Κάθε οργανισμός οφείλει να αξιολογεί συνεχώς τα υπάρχοντα μέτρα

ασφαλείας και να ορίζει τεχνικά και οργανωτικά μέτρα, ώστε να επιτυγχάνεται η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων.

Τα Δεδομένα προσωπικού χαρακτήρα αποθηκεύονται, διαγράφονται ή μεταφέρονται με βάση το «Πλαίσιο Ασφάλειας Πληροφοριών» του κάθε οργανισμού και αυτό γίνεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών και περιλαμβάνει όλες τις διαδικασίες και τις τεχνικές για τον σκοπό αυτόν. Υπάρχουν Νομικές και Θεσμικές απαιτήσεις σχετικά με τη διαμόρφωση ενός πλαισίου ασφαλείας των πληροφοριών (ΑΠΔ, Ασφάλεια επεξεργασίας, 2020).

Συγκεκριμένα, τα υποκείμενα των δεδομένων έχουν το δικαίωμα πρόσβασης και το δικαίωμα φορητότητας στα προσωπικά τους δεδομένα, δωρεάν. Επίσης, εάν κάποιο υποκείμενο δεδομένων πιστεύει ότι τα προσωπικά του δεδομένα είναι εσφαλμένα, ελλιπή ή ανακριβή, έχει το δικαίωμα να ζητήσει τη διόρθωση ή τη συμπλήρωσή τους χωρίς καμία καθυστέρηση. Μπορεί, επίσης, να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των προσωπικών του δεδομένων για μια συγκεκριμένη χρήση, ή να ζητήσει την περιορισμένη επεξεργασία τους. Σε ορισμένες περιπτώσεις μπορεί να ζητηθεί και η διαγραφή των δεδομένων από τον υπεύθυνο επεξεργασίας, για παράδειγμα όταν τα δεδομένα αυτά δεν χρειάζονται πλέον για την επίτευξη του σκοπού της επεξεργασίας.

Η προστασία της ιδιωτικής ζωής ενός ατόμου είναι σημαντική. Με την ψηφιακή τεχνολογία το άτομο διευκολύνεται σημαντικά σε ατομικό και κοινωνικό επίπεδο, για την αποφυγή κινδύνων, όμως, απαιτείται η διασφάλιση των προσωπικών δεδομένων με νόμους και ηθική δεοντολογία.

2.3.1 Η ΕΝΝΟΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η έννοια της ασφάλειας πληροφοριών περιλαμβάνει τη διαθεσιμότητα, την αξιοπιστία και την ακεραιότητα των πληροφοριών, ώστε να επιτυγχάνεται η συνεχής ροή των πληροφοριών με παράλληλη απόκρυψή τους από μη εξουσιοδοτημένους χρήστες. Γι' αυτό οι πληροφορίες πρέπει να είναι πλήρεις, ακριβείς, έγκυρες και οι μηχανισμοί που χρησιμοποιούνται να είναι υπεύθυνοι για την προστασία των πληροφοριών από πιθανούς κινδύνους (ΑΠΔ, Ασφάλεια επεξεργασίας, 2020).

2.3.2 ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

Τα μέτρα ασφαλείας διαχειρίζονται τη διακίνηση των δεδομένων μέσω διαδικτύου. Αυτά είναι: η κρυπτογράφηση, η ανωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα, η αυθεντικοποίηση, η εξουσιοδότηση, δηλαδή η πρόσβαση στα συστήματα, ο έλεγχος της αξιοπιστίας των δεδομένων, με σκοπό την αξιοπιστία και τη διαθεσιμότητα των δεδομένων σε περίπτωση παραβίασης αυτών (ΑΠΔ, Σχέδιο Ανάκαμψης από Καταστροφές, 2022).

2.4 ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΕΠΙΠΤΩΣΕΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Η διενέργεια αξιολόγησης των επιπτώσεων σχετικά με την προστασία δεδομένων (DPIA) είναι υποχρεωτική όταν η επικείμενη επεξεργασία θέτει σε μεγάλο κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, π.χ. κατά τη χρήση νέων τεχνολογιών. Τέτοιος μεγάλος κίνδυνος προκύπτει όταν χρησιμοποιούνται αυτοματοποιημένοι μηχανισμοί επεξεργασίας δεδομένων και δημιουργίας προφίλ ή όταν παρακολουθείται δημόσιος χώρος σε μεγάλη έκταση (π.χ. κάμερες CCTV) και γίνεται επεξεργασία σε μεγάλη κλίμακα, ειδικών κατηγοριών

δεδομένων ή προσωπικών δεδομένων που σχετίζονται με ποινικές καταδίκες και αδικήματα (π.χ. δεδομένα υγείας).

2.5 ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR ΣΕ ΤΟΜΕΙΣ ΚΟΙΝΩΝΙΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ

Για να γίνει κατανοητή η ανάγκη για ένα νέο νομοθετικό πλαίσιο με αντικείμενο την προστασία των προσωπικών δεδομένων, είναι σκόπιμο να εξεταστεί εν συντομία ποιο ήταν το ισχύον καθεστώς της νομοθεσίας που ίσχυε, της ευρωπαϊκής οδηγίας του 1995 για την προστασία προσωπικών δεδομένων, υπό ποιες συνθήκες αυτή συντάχθηκε και ποιες είναι οι διαφορές με τις σημερινές.

Αρχικά, το γεγονός ότι ήταν οδηγία σημαίνει πως η κάθε χώρα την ερμήνευε, ώστε να την υιοθετήσει, με μια σχετική ελευθερία. Η ελευθερία αυτή έγκειται κυρίως στο πώς οι βασιζόμενοι σε αυτή νόμοι θα συντάσσονταν (υπό την προϋπόθεση ότι πληρούσαν τις προαπαιτήσεις, που προέβλεπε η οδηγία). Αυτή η ελευθερία επεκτάθηκε και στο κομμάτι της εφαρμογής αυτών των νόμων. Η έλλειψη νομικών προηγούμενων, καθώς και η δυσκολία στην ενημέρωση και πληροφόρηση γύρω από ζητήματα τεχνολογίας είχε ως αποτέλεσμα μεγάλες αποκλίσεις στην αυστηρότητα εφαρμογής των νόμων και στη βαρύτητα των ποινών ανά χώρα. Το αποτέλεσμα ήταν χαοτικό για οποιονδήποτε προσπαθούσε να λειτουργήσει σε περισσότερα του ενός κράτους – μέλους.

Ταυτόχρονα, η χρήση του διαδικτύου ήταν εξαιρετικά περιορισμένη και ο τρόπος λειτουργίας τόσο του εμπορίου όσο και της παγκόσμιας οικονομίας δεν ήταν σχεδόν καθόλου ψηφιοποιημένος, όπως σήμερα, που θεωρείται αυτονόητο πλέον ότι, όταν ένα σύστημα είναι συνδεδεμένο στο διαδίκτυο, τα δεδομένα του μπορούν εύκολα να διαρρεύσουν. Ο αριθμός των συσκευών, που μπορούν να συνδεθούν στο διαδίκτυο, καθώς και των

εφαρμογών, που αυτό προσφέρει, έχουν αυξηθεί εκθετικά μέσα στις δυο τελευταίες δεκαετίες. Επομένως, ο όγκος των δεδομένων, που μπορούν εν δυνάμει να αντληθούν και να μελετηθούν, είναι μεγαλύτερος από ποτέ. Ανάλογος είναι και ο κίνδυνος τα δεδομένα ενός χρήστη να κυκλοφορήσουν χωρίς την εκπεφρασμένη συγκατάθεσή του.

Ο GDPR δημουργώντας όλες τις αλληλεπιδράσεις μεταξύ χρηστών και οργανισμών στο διαδίκτυο, όπως και τη μεταφορά και επεξεργασία δεδομένων, έχει έμμεσα βρεθεί στη θέση να καθορίζει τη λειτουργία της σύγχρονης κοινωνίας. Αυτό είναι αποτέλεσμα του κομβικού ρόλου που έχει αναλάβει το διαδίκτυο στη μοντέρνα πραγματικότητα, κάτι το οποίο γίνεται εύκολα αντιληπτό αν κάποιος σκεφτεί ότι, για παράδειγμα, η έρευνα για την αντιμετώπιση του COVID απαιτεί ταχεία επικοινωνία μεταξύ ερευνητικών ομάδων, με διεθνή σύνθεση, οι οποίες μοιράζονται δεδομένα τα οποία έχουν συλλεχθεί από εκατομμύρια ασθενείς παγκοσμίως, ή ότι τώρα μέσω του διαδικτύου, όλες οι «έξυπνες» συσκευές επικοινωνούν μεταξύ τους δημιουργώντας το λεγόμενο Internet of Things (IoT) το οποίο φέρει επανάσταση στην τεχνολογία. Άρα, κάλλιστα θα μπορούσε να ισχυριστεί κάποιος ότι η κοινωνία του σήμερα στηρίζεται στα δεδομένα για την εύρυθμη λειτουργία της. Είναι λογικό επακόλουθο ότι ο GDPR βρίσκεται στο προσκήνιο ως λύση των προκλήσεων, που αντιμετωπίζει η ευρωπαϊκή κοινότητα. Έτσι, λοιπόν, δεν θα μπορούσε να λείψει από καμία έρευνα, η μελέτη του αντίκτυπου που είχε ο GDPR στους τομείς της υγείας, των επιχειρήσεων και της ηθικής.

Αυτή η ενότητα εστιάζει στον τομέα της υγείας, ο οποίος βιώνει έναν ραγδαίο ψηφιακό μετασχηματισμό. Ο μετασχηματισμός αυτός αποσκοπεί στο να εξατομικευθεί η υγειονομική περίθαλψη δίνοντας, έτσι, τη βέλτιστη δυνατή θεραπεία στον κάθε ασθενή, μειώνοντας ταυτόχρονα το κόστος της

περίθαλψής του. Η ψηφιοποίηση στηρίζεται στην πρόσφατη και μεγάλη αύξηση του αριθμού των χρηστών έξυπνων συσκευών, οι οποίες έχουν τη δυνατότητα να συλλέγουν τα βιομετρικά δεδομένα του χρήστη τους, δίνοντας έτσι στον θεράποντα ιατρό πολύτιμες πληροφορίες, που βοηθούν στην αντιμετώπιση των διαφόρων προβλημάτων υγείας του ασθενή. Αυτά, όμως, τα δεδομένα λόγω της ιδιαίτερα προσωπικής τους φύσης απαιτούν ειδική μεταχείριση, η οποία ορίζεται από τον GDPR. Για αυτόν το λόγο θα μελετηθεί αν οι περιορισμοί που επιβάλλει ο GDPR πετυχαίνουν να προστατεύσουν την ιδιωτικότητα χωρίς, όμως, να καταπνίγουν τις καινοτόμες αυτές χρήσεις της τεχνολογίας.

Έπειτα θα αναλυθεί η ιδιάζουσα (λόγω της ταχύτητας που απαιτεί η σωστή αντιμετώπισή της) περίπτωση του COVID, κατά την οποία, πολλοί που κυριεύθηκαν από φόβο, πρότειναν να παρακαμφθεί ο GDPR, με σκοπό την επιτάχυνση των ερευνητικών διαδικασιών. Όμως, όπως είχε πει ο διάσημος Αμερικάνος στρατηγός και έπειτα πρόεδρος Eisenhower, κατά την διάρκεια της μεγαλύτερης κρίσης της ιστορίας, τον 2ο Παγκόσμιο Πόλεμο, « … αν κάποιος πολιτισμός θέλει να επιβιώσει πρέπει να ακολουθεί τους κανόνες δικαίου». Έτσι λοιπόν, θα μελετηθούν οι ιδιαίτερες διατάξεις του GDPR, που επιτρέπουν στους ερευνητές τη λήψη της ταχείας και γενικής συγκατάθεσης των ασθενών τους για τη χρήση των προσωπικών δεδομένων τους για έρευνα.

Λόγω της παγκοσμιοποίησης και της πολυεθνικής δομής των σύγχρονων εταιρειών υπάρχει μια συνεχής ανταλλαγή δεδομένων μεταξύ επιχειρήσεων ανεξαρτήτως εθνικών συνόρων. Επιπλέον, ως αποτέλεσμα της αύξησης των χρηστών του διαδικτύου δίνεται η ευκαιρία στις εταιρείες να μελετήσουν τα πολυάριθμα δεδομένα των χρηστών και από την ανάλυση αυτή μπορούν να βγάλουν πολύτιμα συμπεράσματα, που τις

βοηθούν στις διαφημιστικές τους εκστρατείες και στη δημιουργία νέων προϊόντων, που καλύπτουν ανάγκες της αγοράς. Ακόμα και οι μικρομεσαίες επιχειρήσεις έχουν βρει τρόπους να χρησιμοποιήσουν τα προσωπικά δεδομένα για να αυξήσουν τα κέρδη τους. Έχει, επομένως, ιδιαίτερη σημασία να τονιστεί ο αντίκτυπος που είχε η εφαρμογή του GDPR, που ορίζει πώς επιτρέπεται να χρησιμοποιηθούν τα δεδομένα αυτά στις επιχειρήσεις.

Τέλος, θα αναλυθεί η ψηφιακή ηθική, η οποία ασχολείται με τα ηθικά προβλήματα που δημιουργεί η χρήση των δεδομένων και πληροφοριών. Αυτό θα γίνει, διότι η ψηφιακή διακυβέρνηση ως μηχανισμός θέσπισης και εφαρμογής πολιτικών και διαδικασιών που αποσκοπεί στην ανάπτυξη, είναι τομέας που απαιτεί πέρα από την απλή κατανόηση του νόμου και κατανόηση των ηθικών ζητημάτων. Οι αβεβαιότητες που υπάρχουν στον κανονισμό λόγω της πολυπλοκότητάς του είναι ανάγκη να απαντηθούν με τη χρήση της “ήπιας” ηθικής όπως θα φανεί και παρακάτω.

ΚΕΦΑΛΑΙΟ 3: GDPR ΚΑΙ ΥΓΕΙΑ

Ένας από τους τομείς που επηρεάστηκαν έντονα από την εφαρμογή του GDPR ήταν η Υγεία, με την κλινική έρευνα. Η πολυπλοκότητα του κανονισμού απαιτούσε καθοδήγηση των ερευνητικών οργανισμών από τους αρμόδιους φορείς, η οποία όμως ακόμα και μερικούς μήνες πριν την εφαρμογή του δεν ήταν διαθέσιμη σε όλους, ώστε να προετοιμαστούν κατάλληλα. Εν μέρει αυτό εξηγείται από το ευρύ φάσμα των περιπτώσεων που καλύπτει ο κανονισμός αυτός. Είναι μέχρι σήμερα μια από τις πιο εκτεταμένες νομοθετικές πράξεις των πρόσφατων χρόνων και πρωτοπόρα στον τομέα της τεχνολογίας και προστασίας των προσωπικών δεδομένων.

3.1 Η ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR ΣΤΟΝ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ

Ωστόσο, μαζί με την πρωτοπορία έρχεται και η εξερεύνηση του αγνώστου και αυτή ακριβώς ήταν η ανησυχία πολλών ερευνητών καθώς πλησίαζε η ημέρα της υποχρεωτικής εφαρμογής του κανονισμού. Στο επίκεντρο των σκέψεών τους ήταν ο τρόπος με τον οποίο θα μπορέσει ο κανονισμός να επιτύχει τον στόχο του (την προστασία δηλαδή των προσωπικών δεδομένων), χωρίς να διαταράξει την έρευνα, η οποία ήταν και είναι από τη φύση της “παγκόσμια”, δυσχεραίνοντας τη μεταφορά και φύλαξη των δεδομένων.

Ειδικά στο πεδίο της κλινικής μελέτης και έρευνας, τα Δεδομένα του Πραγματικού Κόσμου (Real World Data, RWD) χρησιμοποιούνται κατά κόρον από πολλούς οργανισμούς, συμπεριλαμβανομένων των φαρμακευτικών εταιρειών, και παρέχουν πληθώρα πληροφοριών για τα αποτελέσματα θεραπειών σε ασθενείς. Δεν είναι σπάνιο τέτοια δεδομένα να απαντούν σε ερωτήσεις που δεν είχαν καν τεθεί. Από τη στιγμή που ανακαλύφθηκαν τα ψηφιακά αξεσουάρ υγείας π.χ. τα έξυπνα ρολόγια και έγιναν τόσο δημοφιλή, η συλλογή των RWD εκτινάχθηκε, όπως και

συναφείς τομείς, και απαιτείται η εφαρμογή μιας ερευνητικής τεχνικής εναρμονισμένης με τον κανονισμό, όσον αφορά τη συλλογή δεδομένων από τέτοιες πηγές. Ταυτόχρονα, όμως, οι ιδιοκτήτες των δεδομένων αυτών θέλουν να έχουν τον έλεγχο και να ξέρουν πώς φυλάσσονται, ποια επεξεργασία υφίστανται, πώς χρησιμοποιούνται και ,τελικά, αν μπορούν να διαγραφούν τα στοιχεία αυτά (Becky McCall, 2018).

Σήμερα, μερικά χρόνια μετά την εφαρμογή του GDPR, πολλοί από τους μεγάλους οργανισμούς συμφωνούν πως η τελική μορφή του κανονισμού υποστηρίζει την έρευνα περισσότερο από όσο είχε αρχικά εκτιμηθεί. Για παράδειγμα, η αναγνώριση του ότι τα δεδομένα μπορούν να παραμένουν χρήσιμα ακόμα και χρόνια μετά τη συλλογή τους και πως, ενώ συλλέγονται για έναν σκοπό, μπορούν να φανούν χρήσιμα σε μια πληθώρα από διαφορετικές έρευνες και εφαρμογές, έχει φανεί ιδιαίτερα χρήσιμη. Το δεύτερο ειδικά είναι κρίσιμο στοιχείο, διότι δεδομένα, που συλλέχθηκαν για μια ασθένεια, ενδέχεται να φανεί πως σχετίζονται και με άλλες ασθένειες καθώς οι γνώσεις για αυτές αναπτύσσονται.

Ο κανονισμός επιτρέπει στα μέλη κράτη της Ε.Ε. να παρεκκλίνουν από κάποια δικαιώματα του ιδιοκτήτη των δεδομένων, όταν αυτά πρόκειται να χρησιμοποιηθούν για επιστημονικούς σκοπούς στα πεδία της υγείας, βιομετρίας ή της γενετικής (Becky McCall, 2018). Παρόλα αυτά, εναλλακτικές μέθοδοι ίσως να είναι προτιμητέες καθώς είναι προς το συμφέρον της επιστημονικής κοινότητας και της αποδοτικότητάς της να αποφύγει τη χρήση “εξαιρέσεων” στον κανονισμό ώστε να μπορεί να διεξάγει έρευνα. Αντ' αυτού θα μπορούσε να γίνει χρήση ενός ηπιότερου νομικού εργαλείου, όπως π.χ. ένας Κώδικας Δεοντολογίας που ξεπερνάει εθνικά σύνορα και ενώνει ολόκληρο τον βιοιατρικό και φαρμακευτικό ερευνητικό τομέα. Ελλείψει μιας τέτοιας προσέγγισης, είναι πιθανό πως η

Ε.Ε. θα απομακρυνθεί από έναν από τους στόχους της: την επίτευξη μια κοινής ερευνητικής στρατηγικής στην Ευρώπη.

Ο GDPR ισχύει άμεσα για δεδομένα φροντίδας ασθενών, καθώς και έρευνας. Η πλειονότητα της ιατρικής κοινότητας πιστεύει πως η σχέση γιατρού-ασθενούς βασίζεται στην εμπιστοσύνη. Ως εκ τούτου, οι σαφείς κανόνες που διέπουν την ανταλλαγή πληροφοριών είναι ουσιαστικής σημασίας. Οι βασικές αρχές του GDPR παραμένουν κοινές στον τομέα της υγείας και σε άλλους τομείς εφαρμογής του κανονισμού, ωστόσο, υπάρχουν αυξημένες ευθύνες για τους γιατρούς και τον ρόλο τους ως υπεύθυνων επεξεργασίας δεδομένων. Πρέπει να δοθεί καθοδήγηση η οποία θα βοηθήσει τους γιατρούς να μάθουν πώς μπορούν να διασφαλίσουν τις πρακτικές τους, να τους προετοιμάζουν για τις ευθύνες τους και για τα βήματα που πρέπει να ακολουθήσουν σε κάθε μια από τις εκάστοτε διαδικασίες (Becky McCall, 2018).

Η υγειονομική περίθαλψη υπόκειται ταυτόχρονα στη μετάβαση σε ένα ψηφιακό σύστημα και στην εφαρμογή του νέου Γενικού Κανονισμού Προστασίας των Δεδομένων (GDPR), που εισάγει αλλαγές στη χρήση του διαδικτύου για τους ερευνητές. Η μελέτη του GDPR μπορεί να διευκολύνει τους ενδιαφερόμενους και τους πολιτικούς στη χάραξη πολιτικής στον τομέα της υγειονομικής περίθαλψης στην ψηφιακή εποχή (M. Karampela, S. Ouhbi M.;Isomursu, 2019).

Όραμα των σύγχρονων υγειονομικών συστημάτων είναι, έτσι, να επιτρέψουν την εξατομικευμένη φροντίδα μειώνοντας τις δαπάνες, χωρίς να τεθεί σε κίνδυνο η ποιότητα των υπηρεσιών (J. Koster, E. Stewart;E. Kolker, 2016:165-167). Για την υλοποίηση αυτού του οράματος η ανάγκη για τη χρήση των προσωπικών δεδομένων είναι ξεκάθαρη (W. Raghupathi; V. Raghupathi, 2014:3). Ο εξαιρετικά μεγάλος όγκος πληροφοριών υγείας,

που συλλέγονται καθώς οι άνθρωποι χρησιμοποιούν φορητές συσκευές, κινητούς αισθητήρες και αισθητήρες ζωτικών σημάτων (smartwatches και smartphones) στην καθημερινή τους ζωή, συμβάλλει στην εξατομίκευση της υγειονομικής περίθαλψης. (Y. Wang, L. Kung, W. Y. C. Wang, C. G. Cegielski, 2018:64-79; S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak,2015:678-708; J. C. Willcox, P. van der Pligt, K. Ball, S. A. Wilkinson, M. Lappas, E. A. McCarthy, K. J. Campbell,2015)

Τα πιθανά οφέλη από τη χρήση των προσωπικών δεδομένων υγείας είναι πολυάριθμα. Για παράδειγμα, εντοπίζουν τους κινδύνους υγείας που έχει κάποιος (μειώνοντας το κόστος στην παροχή υγειονομικής περίθαλψης), και συντελούν στη βελτίωση της αποτελεσματικότητας των υπηρεσιών, στη διαχείριση ασθενειών που σχετίζονται με τον τρόπο ζωής ή ακόμα και στην εξερεύνηση νέων θεραπειών για τον καρκίνο (Y. Wang, L. Kung, W. Y. C. Wang, C. G. Cegielski, 2018:64-70; A. K. Green, K. E. Reeder-Hayes, R. W. Corty, E. Basch, M. I.Milowsky, S. B. Dusetzina, A. V. Bennett, W. A. Wood,2015:464-e20). Περαιτέρω εφαρμογές θα μπορούσαν να υπάρχουν για την πρόληψη ασθενειών, όπως μια απλή γρίπη από τη μελέτη των συμπτωμάτων της σε ολόκληρη την Ε.Ε. σε πραγματικό χρόνο, (“Flue Near You,” 2019) ή ακόμα και το HealthMap, μία εφαρμογή για την καταγραφή εστιών μολυσματικών ασθενειών. Αυτά είναι και παραδείγματα πιθανής εμπορικής χρήσης τέτοιων δεδομένων (Healthmap, 2019). Τέτοιες εφαρμογές δεν έχουν μόνο αυξήσει τις απαιτήσεις των χρηστών, αλλά και έχουν επιταχύνει τη δημιουργία πιο ευέλικτων συστημάτων στην υγειονομική περίθαλψη για την κοινή χρήση δεδομένων υγείας (D. D. Vergados, 2020:575-590).

Η προστασία δεδομένων σχετίζεται με την πρόσβαση και την κοινή χρήση των δεδομένων (P. Samarati; S. D. C. Di Vimercati, 2010:1-14). Η εφαρμογή

του νέου Κανονισμού Γενικής Προστασίας Δεδομένων (GDPR) τον Μάιο του 2018 εισήγαγε τους ευρωπαίους πολίτες σε μια νέα εποχή: την εποχή της ενδυνάμωσης των ατομικών δικαιωμάτων και της κοινής λήψης αποφάσεων. Το νέο νομικό πλαίσιο στοχεύει να γεφυρώσει το νομικό κενό που προέκυψε από την εξέλιξη νέων τεχνολογιών, καθώς και στην εναρμόνιση των νόμων που προϋπήρχαν στα κράτη μέλη της Ε.Ε. (B. Custers, F. Dechesne, A. M. Sears, T. Tani; S. van der Hof, 2018:234-243). Σε παγκόσμιο επίπεδο σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας (ΠΟΥ), μόνο το 34% των κρατών μελών ανέφερε ότι εφαρμοζόταν ανταλλαγή δεδομένων, η οποία ήταν νόμιμη εντός της ίδιας της χώρας, και μόνο 22% έκανε λόγο για διεθνή ανταλλαγή δεδομένων (World Health Organization, 2016).

Ως εκ τούτου, η εναρμόνιση της νομοθεσίας σε παγκόσμιο επίπεδο είναι ακόμα σε στάδιο ανάπτυξης. Οι μεταβολές στην τεχνολογία και η αλλαγή που αυτή επιφέρει στη συμπεριφορά των χρηστών της, έχουν μελετηθεί από πολλές οπτικές γωνίες, για παράδειγμα από το τεχνολογικό μοντέλο αποδοχής ή τη θεωρία της αιτιολογημένης δράσης (M. Fishbein and I. Ajzen, 1975 & V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, 2003:425-478). Και οι δύο θεωρίες υποστηρίζουν ότι οι χρήστες αναπτύσσουν συγκεκριμένες στάσεις προς την τεχνολογία, αλλά και ότι υπάρχει μια σχέση μεταξύ των στάσεων και του νομικού πλαισίου (I. Ajzen, 1991 & F. D. Davis and P. R. Warshaw,1992 & S. Taylor and P. A. Todd, 1995).

Οι συγγραφείς της έρευνας «Διερεύνηση της προθυμίας των χρηστών να μοιραστούν την υγεία και τα προσωπικά τους δεδομένα κάτω από το πρίσμα του νέου GDPR: επιπτώσεις στην υγειονομική περίθαλψη» ήθελαν να μελετήσουν τον τρόπο, με τον οποίο ο GDPR επηρέασε τον τομέα της

υγείας, μελετώντας την ύπαρξη (ή μη) αλλαγών στην πρόθεση των ατόμων να μοιραστούν προσωπικά δεδομένα έπειτα από την θέσπιση του GDPR, που για πρώτη φορά τους έδινε την δυνατότητα να επιλέξουν (I. Ajzen, 1991:181).

Έτσι, ανέλυσαν τα αποτελέσματα ενός ερωτηματολογίου για τη διερεύνηση της προθυμίας 8.004 ατόμων σε τέσσερις ευρωπαϊκές χώρες στην κοινή χρήση τεσσάρων τύπων δεδομένων: υγεία, αξίες και πεποιθήσεις, καταναλωτικές συνήθειες-αγορές και οικονομική ευμάρεια. Τα αποτελέσματα υποδηλώνουν ότι οι συμμετέχοντες είναι πιο πρόθυμοι να μοιραστούν δεδομένα υγείας και δεδομένα σχετικά με τις πεποιθήσεις και τις αξίες τους παρά πληροφορίες για την περιουσία τους και ότι ο GDPR έχει επηρεάσει την ευκολία ανταλλαγής δεδομένων.

Η συλλογή δεδομένων πραγματοποιήθηκε από 6 έως 18 Δεκεμβρίου 2018 σε 4 ευρωπαϊκές χώρες: Φινλανδία, Ολλανδία, Γερμανία και Γαλλία. Η έρευνα αποτελείτο από ερωτήσεις που αφορούν τη συλλογή δεδομένων, τα οποία σχετίζονται με το ιατρικό ιστορικό των ερωτηθέντων, τις ιατρικές υπηρεσίες και την εμπιστοσύνη προς τις υπηρεσίες αυτές για τη σωστή διαχείριση δεδομένων. Εξέτασαν δύο ερωτήσεις: 1. Πώς έχει ο ευρωπαϊκός GDPR επηρεάσει τη συμπεριφορά και τη θέλησή τους να διαθέσουν στοιχεία σε σχέση με τα τέσσερα είδη προσωπικών δεδομένων και 2. Είναι οι χρήστες πρόθυμοι να μοιράζονται δεδομένα υγείας περισσότερο από άλλα είδη δεδομένων;

Σε αυτή τη μελέτη, τα προσωπικά δεδομένα αναφέρονται σε τέσσερις τύπους δεδομένων: υγείας ή κληρονομικότητας, αξίες και πεποιθήσεις, καταναλωτικές συνήθειες ή αγορές και τον πλούτο (οικονομικά). Σύμφωνα με την έρευνα, λοιπόν, είδαμε ότι οι χρήστες θα ήταν πρόθυμοι να μοιραστούν δεδομένα σχετικά με την κατανάλωση και τις αγορές τους,

ωστόσο ήταν πολύ απρόθυμοι να αποκαλύψουν δεδομένα περί των οικονομικών τους. Οι νεότεροι μοιράζονται περισσότερο τα δεδομένα τους από τους γηραιότερους (οι πιο ηλικιωμένοι) συμμετέχοντες. Περίπου δύο στους τρεις χρήστες ήταν πρόθυμοι να μοιραστούν πληροφορίες σχετικά με τις αξίες και τις πεποιθήσεις τους, και δεδομένα περί ιστορικού υγείας και κληρονομικότητας. Η ευκολία που δείχνουν οι ερωτηθέντες στο να μοιραστούν τις αξίες και τα πιστεύω τους δεν είναι απροσδόκητο εύρημα, αν αναλογιστεί κανείς ότι οι άνθρωποι συχνά μοιράζονται προσωπικές αξίες στα μέσα κοινωνικής δικτύωσης.

Ένα ενδιαφέρον εύρημα είναι ότι ο πιο ευαίσθητος τύπος δεδομένων είναι τα δεδομένα πλούτου. Η ιδέα του "αλτρουισμού" δεδομένων θα μπορούσε ενδεχομένως να εξηγήσει την προθυμία των συμμετεχόντων να μοιράζονται τα δεδομένα υγείας τους, ως χρήστες, αφού συχνά πιστεύουν ότι η κοινοποίηση των δεδομένων υγείας τους θα μπορούσε να συμβάλει στην βελτίωση της υγείας του γενικού πληθυσμού. Σύμφωνα με το IBM Big data & analytics Hub, 4,9 εκατομμύρια χρήστες παγκοσμίως θα μπορούσαν να έχουν νοσηλευτεί εκτός νοσοκομείου αν παρακολουθούνταν με χρήση αισθητήρων (BM Big data and analytics Hub, 2019). Ηλεκτρονικές εφαρμογές οι οποίες μπορούν για παράδειγμα να στέλνουν ειδοποιήσεις σε πραγματικό χρόνο για την παρακολούθηση του άσθματος, (Asthmapolis,2019) ταυτοποίηση των παραγόντων κινδύνου για κατάχρηση απιοειδών (Fuzzy Logix, 2019) και ανακάλυψη νέων φαρμάκων για τη θεραπεία του καρκίνου του πνεύμονα,(Stanford Medice,2019) είναι μεταξύ των εφαρμογών που έχουν φανεί ότι είχαν θετικό αντίκτυπο στη ζωή των ανθρώπων. Τα δεδομένα υγείας έχουν τεράστια οικονομική αξία. Η χρήση του blockchain στην υγειονομική περίθαλψη δεν είναι ένα πλασματικό σενάριο αλλά ένα πιθανό μέλλον. Το CoverUS πληρώνει τους καταναλωτές

για την πώληση των δεδομένων υγείας τους με ένα κρυπτονόμισμα που ονομάζεται CoverCoin (CoverUS, 2019).

Άλλα παραδείγματα είναι η εταιρεία Miinome με έδρα τις ΗΠΑ, στην οποία οι πελάτες μπορούν να "εξαργυρώνουν" το DNA τους με αντάλλαγμα συστάσεις στον τρόπο ζωής τους, ή το "Hub of all Things", στο οποίο οι χρήστες μπορούν να αποθηκεύουν και να ανταλλάσσουν τα προσωπικά τους δεδομένα με αντάλλαγμα «μελέτη και ανάλυση των στοιχείων τους από αλγόριθμους που τους παρέχουν πληροφορίες σχετικά με την υγεία τους, το ιστορικό και τις αναμνήσεις τους» (Miinome, 2019 & T. Hub, 2019). Η αναβάθμιση, που εισήχθη μετά την εφαρμογή του GDPR σε αυτές τις εταιρείες, απαιτεί να ενημερώνουν τους χρήστες τους για την περαιτέρω χρήση των στοιχείων τους αυτών, πράγμα το οποίο θα μπορούσε να έχει θετική επίδραση στην προθυμία των χρηστών να μοιραστούν τα δεδομένα τους, αφού θα ξέρουν για τι χρησιμοποιούνται (E. R. Weitzman, L. Kaci, and K. D. Mandl, 2010 & K. K. Kim, P. Sankar, M. D. Wilson, and S. C. Haynes,2017:25 & J. Kaye, L. Curren, N. Anderson, K. Edwards, S. M. Fullerton, N. Kanellopoulou, D. Lund, D. G. MacArthur, D. Mascalzoni, J. Shep-Herd, 2012:371). Ωστόσο, θα πρέπει να λάβουμε υπόψη ότι η συναίνεση συμμετοχής στον GDPR εμφανίζεται τόσο συχνά σε ιστοσελίδες και εφαρμογές των κινητών τηλεφώνων, που είναι πιθανό οι χρήστες να μη διαβάζουν σε τι συναινούν και απλώς να συμφωνούν, παραιτούμενοι έτσι από τα δικαιώματα επί του απορρήτου τους.

Μετά την εφαρμογή του GDPR περισσότερο από το ένα τρίτο των συμμετεχόντων (36% κατά μέσο όρο) ανέφερε ότι η επιβολή του GDPR δεν είχε καμία επίδραση στη συμπεριφορά τους. Αν και το χρονοδιάγραμμα αυτής της μελέτης μετά την επιβολή του νέου GDPR είναι σύντομο, θα μπορούσε να υποστηριχτεί ότι η φασαρία στα δίκτυα κοινωνικής δικτύωσης

γύρω από την νέα νομοθεσία και τη λήψη πολυάριθμων emails από εταιρείες και οργανισμούς σχετικά με νέα cookies και τη συναίνεση φαίνεται να έχει επηρεάσει τη στάση των χρηστών.

Αλλά, για να αλλάξουν τη συμπεριφορά τους οι χρήστες απαιτείται να έχουν γνώση των δικαιωμάτων τους. Λαμβάνοντας υπόψη ότι οι πολιτικές απορρήτου συχνά αποτυγχάνουν να κοινοποιούν τους κινδύνους που ενέχει η σύνδεση και επεξεργασία δεδομένων, οι χρήστες δεν αντιλαμβάνονται των έμπρακτων αποτελεσμάτων που έχει στην καθημερινή ζωή η κοινή χρήση των δεδομένων τους (S. Wachter,2018:436-449).

Κάποιοι εξέφρασαν μια σειρά από επιφυλάξεις σχετικά με τη λειτουργία του GDPR. Δηλαδή ότι είναι μια αυταπάτη , ότι τα άτομα δεν θα έχουν τον έλεγχο των δεδομένων τους και ότι θα αποδειχθούν ψευδείς οι προσδοκίες τους για εφαρμογή του δικαίου (B.-J. Koops, 2014:250-261).

Τα δεδομένα υγείας είναι απαραίτητα για την παροχή εξατομικευμένων υπηρεσιών, την προληπτική φροντίδα και τη δημιουργία ενός βιώσιμου συστήματος υγειονομικής περίθαλψης. Μια πρόκληση για τη μελλοντική υγειονομική περίθαλψη είναι οι χρήστες να κατανοήσουν τα δικαιώματά τους, τους κινδύνους αλλά και τα οφέλη που υπάρχουν με το να διαθέσουν τα δεδομένα τους. Θα μπορούσαν επίσης να απλοποιηθούν οι δηλώσεις απορρήτου, ώστε να συμβάλουν σε αυτό. Οι πολιτικοί θα πρέπει να διασφαλίζουν την υπεύθυνη και ηθική χρήση των προσωπικών υγειονομικών δεδομένων. Τα αποτελέσματα αυτής της μελέτης υποδηλώνουν επίσης ότι ο GDPR έχει επηρεάσει τη συμπεριφορά αρκετών αλλά όχι όλων των συμμετεχόντων όσον αφορά την κοινή χρήση δεδομένων.

ΚΕΦΑΛΑΙΟ 4: GDPR ΚΑΙ COVID – 19

Ο κόσμος αναμένει με ανυπομονησία τους ερευνητές στον τομέα της υγείας να αναπτύξουν αποτελεσματικά εργαλεία που θα βοηθήσουν στην αντιμετώπιση του Covid-19 όπως τεστ, εμβόλια και θεραπείες. Η συλλογή, η ανάλυση και η ταχεία μεταφορά δεδομένων υγείας είναι καίριας σημασίας για τον συντονισμό αυτής της άνευ προηγουμένου διεθνούς προσπάθειας για διεθνή έρευνα (Sharing research data and findings relevant to the novel coronavirus (COVID-19) outbreak, 2020). Ωστόσο, οι νόμοι περί προστασίας των προσωπικών δεδομένων δεν πρέπει να ανασταλούν ακόμα και κατά τη διάρκεια συνθηκών εκτάκτου ανάγκης (όπως στην περίπτωση μιας πανδημίας) (Pierucci A, Walter JP, 2020). Πολλές μορφές ερευνών επί του Covid-19 περιλαμβάνουν την επεξεργασία προσωπικών δεδομένων, συμπεριλαμβανομένων προσωπικών δεδομένων υγείας ή και των γενετικών δεδομένων.

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation, GDPR) (Regulation 2016/679 of the European Parliament, 2016) ρυθμίζει την επεξεργασία των προσωπικών δεδομένων στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ), ο οποίος περιλαμβάνει 27 κράτη μέλη της Ευρωπαϊκής Ένωσης καθώς επίσης και την Ιρλανδία, το Λιχτενστάιν και τη Νορβηγία. Εδώ αξίζει να σημειωθεί ότι Το Ηνωμένο Βασίλειο, κατόπιν της μεταβατικής περιόδου του Brexit, θα διατηρήσει τον GDPR σε τροποποιημένη μορφή, εντούτοις οι τροποποιήσεις αυτές δεν έχουν αλλάξει τις βασικές αρχές του (European Union (Withdrawal) Act, 2018 & The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations, 2019). Κατ’ αρχάς, ο GDPR παρέχει ένα σύνολο εργαλείων για την επεξεργασία προσωπικών δεδομένων κατά

τη διάρκεια μιας κρίσης υγείας, συμπεριλαμβανομένης και της έρευνας για θέματα υγείας (European Data Protection Board, 2020).

Ένας από τους βασικότερους λόγους για την υιοθέτηση του GDPR και την αντικατάσταση του προκατόχου του (την Επιτροπή Προστασίας Δεδομένων) (Directive 95/46/EC, 1995) ήταν να δημιουργήσει ένα εναρμονισμένο καθεστώς προστασίας σε ολόκληρο τον ΕΟΧ (Kuner C, Bygrave L, Docksey C., 2020:1-47). Ωστόσο, μια σημαντική αδυναμία του GDPR είναι ότι η ερμηνεία πολλαπλών διατάξεων περί δημόσιας υγείας όσο και άλλων σχετικών με την υγεία διατάξεων μένει ανοιχτή στα επιμέρους εθνικά νομοθετικά σώματα. Κατά συνέπεια, οι χώρες έχουν τις δικές τους ξεχωριστές λύσεις και απαιτήσεις σε όποιες περιπτώσεις χρησιμοποιούνται και τυγχάνουν επεξεργασίας προσωπικά δεδομένα (ειδικά εκείνα που αφορούν την υγεία ή τα γενετικά δεδομένα).

Πιο συγκεκριμένα, οι ερευνητικοί φορείς θα πρέπει να έχουν υπόψιν την τριπλή εξουσιοδότηση που χρειάζονται υπό τον GDPR για διεθνή διαμοιρασμό δεδομένων: πρώτον, θεμιτό λόγο για επεξεργασία προσωπικών δεδομένων σύμφωνα με τον κανονισμό, δεύτερον, έγκριση της επεξεργασίας δεδομένων ειδικών κατηγοριών (π.χ. υγείας και γενετικών δεδομένων) και τρίτον, πρακτικό λόγο για μεταφορά τους εκτός του ΕΟΧ. Άλλα σημαντικά πράγματα, που πρέπει να ληφθούν υπόψιν από τα ερευνητικά ιδρύματα, περιλαμβάνουν τον σεβασμό της ιδιωτικότητας των ατόμων από τα οποία συλλέχθηκαν τα δεδομένα και την εξασφάλιση των κατάλληλων δικλείδων ασφαλείας.

Μια βασική αρχή της προστασίας δεδομένων είναι ότι όλα τα προσωπικά δεδομένα θα πρέπει να τυγχάνουν νόμιμης επεξεργασίας. Με άλλα λόγια ένας ερευνητικός οργανισμός θα πρέπει να έχει μια εξουσιοδότηση για να επεξεργάζεται τέτοια δεδομένα, την οποία έχει λάβει με βάση τον GDPR. Οι

δύο πιο σημαντικοί (για την έρευνα υγείας) τρόποι για να λάβει τέτοια εξουσιοδότηση είναι βάσει συγκατάθεσης ή βάσει δημόσιου συμφέροντος. Ας ρίξουμε όμως μια ματιά στα υπέρ και στα κατά του καθενός από τους δύο τρόπους υπό το πρίσμα της ερευνητικής προσπάθειας κατά τη διάρκεια μίας πανδημίας.

Με την πρώτη ματιά, η συγκατάθεση φαίνεται να είναι μια απλή λύση για την επεξεργασία προσωπικών δεδομένων στην έρευνα για τον COVID-19, καθώς είναι σύμφωνη με τις αρχές της ερευνητικής δεοντολογίας. Η συγκατάθεση σύμφωνα με τον GDPR, ωστόσο, θεωρείται ότι είναι εννοιολογικά και λειτουργικά διαφορετική από την ενημερωμένη συγκατάθεση, που γενικά απαιτείται από την ερευνητική ηθική (European Data Protection Supervisor, 2020). Η συναίνεση σύμφωνα με τον GDPR πρέπει να δίνεται ελεύθερα, συγκεκριμένα, ενημερωμένα και ξεκάθαρα, και να μπορεί να αποσυρθεί ανά πάσα στιγμή. Αν και αυτό ουσιαστικά συμφωνεί με τις αρχές της ηθικής, οι Ευρωπαϊκές αρχές προστασίας δεδομένων έχουν ερμηνεύσει αυτά τα τέσσερα στοιχεία συναίνεσης αυστηρά (European Data Protection Board, 2020). Στις περιπτώσεις όπου ζητείται συγκατάθεση κατά τη συλλογή δεδομένων στο πλαίσιο της υγειονομικής περίθαλψης, οι ασθενείς μπορεί να θεωρηθούν ως ευάλωτα άτομα και η συναίνεση ενδέχεται να μην είναι έγκυρη σύμφωνα με τον GDPR, λόγω της μη ισότιμης σχέσης μεταξύ του υπεύθυνου επεξεργασίας των δεδομένων και του υποκειμένου, δηλαδή του ασθενή στην προκειμένη περίπτωση (European Data Protection Board, 2020).

Πρόσφατες οδηγίες από την Ευρωπαϊκή Προστασία Δεδομένων του διοικητικού συμβουλίου (EDPB) προτείνουν η συναίνεση για μη “παρεμβατική” έρευνα όταν αποκτάται από τους ερευνητές, να θεωρείται νόμιμη εφόσον δεν υπάρχει πίεση ή απειλή (European Data Protection

Board Guidelines 05/2020, 2020). Ωστόσο, το EDPB δεν διευκρινίζει εάν αυτή η οδηγία θα επηρεαστεί από τον βαθμό της σοβαρότητας της ασθένειας ή από το αν η συγκατάθεση λαμβάνεται από τον θεράποντα ιατρό. Ερευνητές συχνά θέλουν να αναλύσουν δεδομένα που έχουν συλλεχθεί στο παρελθόν, κάτι ιδιαίτερα συχνό κατά τη διάρκεια μιας πανδημίας. Το θέμα της συναίνεσης σχετικά με τη δευτερογενή χρήση δεδομένων υγειονομικής περίθαλψης για έρευνα αποτελεί μια ιδιαίτερη πρόκληση. Εάν τα δεδομένα είχαν αρχικά συλλεχθεί μόνο για λόγους περίθαλψης, θα ήταν γενικά απαραίτητο να ερωτηθούν ξανά τα υποκείμενα των δεδομένων και να ληφθεί εκ νέου η συγκατάθεσή τους για την επεξεργασία των δεδομένων τους για ερευνητικούς σκοπούς. Οποτεδήποτε οι άνθρωποι βρίσκονται σε κρίσιμη κατάσταση υγείας, κάτι που ισχύει για τους περισσότερους νοσηλευόμενους ασθενείς COVID-19, η λήψη συναίνεσης μπορεί να μην είναι πρακτικά δυνατή.

Επιπλέον, οι ιατροί κατά τη διάρκεια μίας πανδημίας έχουν τεράστιο φόρτο εργασίας. Έτσι λοιπόν είναι δύσκολο για αυτούς να βρουν χρόνο για να παρέχουν τις απαραίτητες πληροφορίες στους ασθενείς, ώστε να ισχύει η συγκατάθεσή τους. Επιπροσθέτως, το προσωπικό που προσεγγίζει ασθενείς για συναίνεση έχει αυξημένο κίνδυνο μόλυνσης, εκτός εάν χρησιμοποιούνται καινοτόμες λύσεις, όπως η ηλεκτρονική συναίνεση. Η απαίτηση να δίνεται συναίνεση για την κάθε χρήση συγκεκριμένα είναι άλλη μια πρόκληση αυτού του κανονισμού. Ένα είδος “ευρείας” συναίνεσης για ερευνητικούς σκοπούς, που σχετίζονται με την πανδημία, είναι δυνατή σύμφωνα με την αιτιολογική σκέψη 33 του GDPR, η οποία συγκεκριμένα αναφέρει ότι «... στους κατόχους των δεδομένων θα πρέπει να επιτρέπεται να δίνουν τη συγκατάθεσή τους σε ορισμένους τομείς της επιστημονικής έρευνας σε συνάρτηση με αναγνωρισμένα δεοντολογικά πρότυπα, αν ο σκοπός είναι η επιστημονική έρευνα». Ωστόσο, ορισμένες

αρχές προστασίας δεδομένων ενδέχεται να μην αποδέχονται τέτοιους σκοπούς ως ικανοποιητικούς και να απαιτούν μια μεταγενέστερη έγκριση μεμονωμένων ερευνητικών σχεδίων.

Πράγματι, οι κατευθυντήριες γραμμές του EDPB σχετικά με τη συναίνεση αναφέρουν ότι, όταν πρόκειται για ερευνητικούς σκοπούς που δεν μπορούν να προσδιοριστούν πλήρως, θα πρέπει να βρεθούν άλλοι τρόποι για να διασφαλιστεί το έγκυρο της συγκατάθεσης που παρέχεται (π.χ. μέσω πρόσθετων συγκαταθέσεων για τα εκάστοτε επόμενα βήματα της έρευνας) (European Data Protection Board, 2020). Αντίθετα, κάποιοι ερευνητές (Hallinan D, 2020) υποστηρίζουν ότι η ευρεία συναίνεση μπορεί να εξακολουθεί να δίνεται σε ορισμένους τομείς έρευνας, όπως η γονιδιωματική. Εν όψει αυτής της θεώρησης, είναι ιδιαίτερα ατυχές το γεγονός ότι οι κατευθυντήριες γραμμές του EDPB για τον COVID-19 και την έρευνα δεν αναφέρουν ότι η ευρύτερη συναίνεση είναι θεμιτή για έρευνα σε πανδημίες. Με βάση την ίδια λογική, που οι αρχές προστασίας δεδομένων επιμένουν σε πρόσθετες συναινέσεις αντί για ευρεία συναίνεση, θέλουν και να περιορίσουν τους σκοπούς και την επεξεργασία δεδομένων για έρευνα.

Με βάση την προϋπόθεση ότι η επεξεργασία που θα γίνει για την έρευνα δεν είναι ασυμβίβαστη με τον αρχικό σκοπό, τότε τα δεδομένα ενδέχεται να υποβληθούν σε περαιτέρω επεξεργασία (πάντα με τις κατάλληλες δικλείδες ασφαλείας). Σε καταστάσεις όπου η συναίνεση είναι η θεμέλια νομική βάση, αυτή η διεύρυνση των σκοπών που μπορεί να χρησιμοποιηθεί για έρευνα είναι πολύ σημαντική. Χωρίς αυτή τη διεύρυνση, η δευτερογενής χρήση των δεδομένων για ερευνητικούς σκοπούς απαιτεί πάντα τη συγκατάθεση που λαμβάνεται από το υποκείμενο των δεδομένων. Ωστόσο, σε περίπτωση συναίνεσης, ενδέχεται οι αρχές

προστασίας δεδομένων να απαιτήσουν εκ νέου συναίνεση, όπως αναφέρεται για παράδειγμα από το Γραφείο Ενημέρωσης Επιτρόπου του Ηνωμένου Βασιλείου.

Τελευταίο, αλλά εξίσου σημαντικό, είναι ότι αποτέλεσμα του ότι η συναίνεση είναι η νομική βάση των δεδομένων, ο κάτοχος των δεδομένων διατηρεί το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Διαφορετικά, ο σεβασμός της αυτόνομης απόφασης του ατόμου αυτού, δεν θα είχε νόημα. Αν η συγκατάθεση που χρησιμεύει ως νομική βάση για την επεξεργασία των δεδομένων αποσυρθεί, η επεξεργασία πρέπει γενικά να σταματήσει και τα δεδομένα πρέπει να διαγραφούν. Η επεξεργασία μπορεί να συνεχιστεί μόνο για άλλους σκοπούς βάσει χωριστής νομικής βάσης που ενδεχομένως έχει ήδη δημιουργηθεί. Το EDPB έχει επισημάνει σε πολλές περιπτώσεις ότι ένας υπεύθυνος επεξεργασίας δεδομένων δεν μπορεί να αλλάξει τη νομική βάση με μια άλλη κατόπιν απόσυρσης της συγκατάθεσης (European Data Protection Board. Guidelines, 2020). Αυτή η θέση φαίνεται να έρχεται σε αντίθεση με το άρθρο GDPR 17, παράγραφος 3 στοιχείο δ, το οποίο περιορίζει το δικαίωμα διαγραφής στις περιπτώσεις που αυτό καθιστά αδύνατη ή βλάπτει σοβαρά την έρευνα.

Για μακροχρόνιες ερευνητικές μελέτες, η διαγραφή μεμονωμένων συνόλων δεδομένων ενδέχεται να μην καταστήσει την έρευνα αδύνατη, αν και οποιαδήποτε επανάληψη αναλύσεων θα μπορούσε να είναι μη πρακτική. Για μεμονωμένες ερευνητικές μελέτες, ωστόσο, η κατάσταση είναι διαφορετική, καθώς αλλάζει σοβαρά η βάση δεδομένων και μπορεί να υπονομεύσει την επιστημονική της αναπαραγωγικότητα. Δεδομένης της δυσκολίας απόκτησης έγκυρης συγκατάθεσης από τους ασθενείς με COVID-19 και την ασάφεια γύρω από τις συνέπειες για ανάκληση της συγκατάθεσης, είναι επιθυμητή μια εναλλακτική νομική βάση σε πολλές

καταστάσεις κατά την επεξεργασία προσωπικών δεδομένων για έρευνα κατά τη διάρκεια αλλά και μετά την κρίση του COVID-19.

Καθώς η επιστημονική έρευνα για τον COVID-19 ωφελεί συλλογικά την κοινωνία , το να χρησιμοποιήσουμε τη νομική βάση ότι είναι μια διεργασία που εκτελείται στο πλαίσιο του κοινού συμφέροντος φαίνεται να είναι μια φυσική επιλογή. Για αυτό είναι η επιλογή που προτείνεται από το EDPB ως ο πιο κατάλληλος τρόπος, ώστε να γίνει λήψη συγκατάθεσης για τη χρήση δεδομένων σε κλινικές δοκιμές και έρευνα (European Data Protection Board Opinion 3/2019, 2019). Η νομική βάση (ότι γίνεται για το δημόσιο συμφέρον), ωστόσο, πρέπει να θεσπιστεί από τη νομοθεσία της Ένωσης ή του κράτους μέλους.

Οι νόμοι περί μολυσματικών ασθενειών ή δημόσιας υγείας μπορούν να παρέχουν την απαραίτητη νομική βάση, ώστε να θεσπιστούν τέτοιες αλλαγές στη νομοθεσία. Σε όποιες περιπτώσεις η νομοθεσία για τις μολυσματικές ασθένειες δεν εξουσιοδοτεί ένα κοινό ερευνητικό ίδρυμα ή πανεπιστήμιο για την επεξεργασία προσωπικών δεδομένων για έρευνα στην πανδημία, ίσως αυτά να είναι σε θέση να βασιστούν στο ότι εκτελούν ερευνητικές αποστολές που τους έχουν ανατεθεί από τον νόμο. Μερικές χώρες, όπως η Φινλανδία (Tietosuojalaki, 2018) και η Νορβηγία (Lov om behandling av personopplysninger, 2018), έχουν καθορίσει στην εθνική τους νομοθεσία ότι μπορεί να γίνει επίκληση της νομικής βάσης δημοσίου συμφέροντος οπουδήποτε η επεξεργασία είναι απαραίτητη για επιστημονικούς σκοπούς.

Συνολικά, η διενέργεια μιας εργασίας για το κοινό συμφέρον μπορεί επίσης να επιτρέπει άλλες παρεκκλίσεις, όπως αυτές που περιγράφονται στα Άρθρα 20 παράγραφος 3 και 21 παράγραφος 6. Ως εκ τούτου, η νομική βάση δημοσίου συμφέροντος μπορεί να επιτρέψει μεγαλύτερη ευελιξία,

ανάλογα με τους όρους υλοποίησης. Είναι επίσης σημαντικό να συνειδητοποιήσει κανείς ότι το άρθρο 6 παράγραφος 1 στοιχείο ε, όπως και κάθε άλλη νομική βάση εκτός συναίνεσης, θα απαιτήσει περαιτέρω εφαρμογή της εθνικής νομοθεσίας του Άρθρου 9 για την επεξεργασία ειδικών κατηγοριών δεδομένων, όπως φαίνεται παρακάτω.

4.1 ΠΕΡΑΙΤΈΡΩ ΝΟΜΙΚΕΣ ΒΑΣΕΙΣ ΣΤΟ ΑΡΘΡΟ 6

Σε καταστάσεις όπου οι θεσμοί δεν μπορούν να βασιστούν στο δημόσιο συμφέρον, είναι θεμιτό το ενδιαφέρον μας για μια άλλη επιλογή, αλλά υπό την προϋπόθεση να διασφαλιστεί ότι η ανάγκη για την επεξεργασία υπερτερεί του απορρήτου του υποκειμένου των δεδομένων και ότι υπάρχει διαφάνεια στην επεξεργασία τους (άρθρο 6[1][στ]). Υπάρχουν και άλλες επιλογές που ισχύουν στο πλαίσιο της υγειονομικής περίθαλψης, αλλά δεν επεκτείνονται για έρευνα:

1. Το άρθρο 6 παράγραφος 1γ υποστηρίζει την επεξεργασία για την εκπλήρωση μιας νομικής υποχρέωσης, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας. Αυτή η βάση καλύπτει την αναφορά του αριθμού των ατόμων που νόσησαν και συνοδευτικά προσωπικά στοιχεία σε περιπτώσεις λοιμωδών νοσημάτων, καθώς και την επεξεργασία δεδομένων από τις αρχές υγείας.

2. Το άρθρο 6 παράγραφος 1 στοιχείο δ εγκρίνει την επεξεργασία εντός του ζωτικού ενδιαφέροντος του κατόχου των δεδομένων ή άλλου φυσικού προσώπου. Ως ζωτικό ενδιαφέρον ερμηνεύονται αυστηρά τα άμεσα ενδιαφέροντα ζωής του υποκειμένου των δεδομένων. Το να βασιζόμαστε σε αυτό το άρθρο για έρευνα είναι πολύ κερδοσκοπικό: η έρευνα στοχεύει στην παραγωγή γενικευμένων γνώσεων και τελικά στοχεύει προς το όφελος της δημόσιας υγείας της ευρύτερης κοινωνίας.

Επομένως, δεν μπορεί να επιτευχθεί για το ζωτικό ενδιαφέρον του ενός ατόμου.

Το άρθρο 6 παράγραφος 1 στοιχείο δ μπορεί να αποτελέσει έγκυρη βάση σε ένα πλαίσιο θεραπείας και θα μπορούσε ακόμη και να παρέχει μια επιλογή παρακολούθησης ατόμων και ενημέρωσής τους σχετικά με έναν πιθανό κίνδυνο μόλυνσης, εάν η ασθένεια είναι επικίνδυνη για τη ζωή. Στο "Γνώμη σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας δεδομένων", η ομάδα εργασίας του άρθρου 29 παραδέχεται ότι το «ζωτικής σημασίας ενδιαφέρον» καλύπτει την επεξεργασία προσωπικών δεδομένων για την προειδοποίηση των ατόμων σχετικά με πιθανή μόλυνση κατά τη διάρκεια μιας επιδημίας, όμως προειδοποιεί ότι δεν πρέπει να αποτελεί τη βάση για μαζική συλλογή ή επεξεργασία προσωπικών δεδομένων. Για αυτόν το λόγο, αυτή η νομική βάση δεν συζητείται καν στην πρόσφατη δήλωση του EDPB σχετικά με τα δεδομένα τοποθεσίας και την ανίχνευση επαφών (European Data Protection Board. Guidelines 04/2020, 2020).

Η αιτιολογική σκέψη 50 του GDPR (gdpr-text, 2020) αναφέρει ότι, όταν υπάρχει περαιτέρω επεξεργασία και αυτή είναι συμβατή με τον αρχικό σκοπό, «... δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των δεδομένων προσωπικού χαρακτήρα.». Αυτό φαίνεται να υποδηλώνει ότι τα δεδομένα, που αρχικά δεν συλλέχθηκαν για ερευνητικούς σκοπούς (π.χ. στο πλαίσιο της υγειονομικής περίθαλψης), μπορεί επίσης να υποβληθούν σε επεξεργασία για έρευνα ,βάσει της αρχικής νομικής βάσης με την οποία συλλέχθηκαν. Για τη συμβατότητα των σκοπών, το άρθρο 5 παράγραφος 1 στοιχείο β λέει ότι η χρήση με σκοπό την επιστημονική έρευνα «...δεν... πρέπει να θεωρείται (ασύμβατη με τον αρχικό σκοπό συλλογής των πληροφοριών) περαιτέρω επεξεργασία»,

εφόσον υπάρχουν κατάλληλες διασφαλίσεις (π.χ. αυτές που καθορίζονται από το άρθρο 89[1]).

Ο βαθμός στον οποίο αυτές οι διατάξεις μπορούν να εφαρμοστούν πέραν του αρχικού ελεγκτή ερμηνεύεται αμφιλεγόμενα. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων αναφέρει στην Προκαταρκτική του Γνώμη, σχετικά με την προστασία δεδομένων και την επιστημονική έρευνα, ότι το άρθρο 5 παράγραφος 1 στοιχείο β δεν παρέχει γενική εξουσιοδότηση για περαιτέρω επεξεργασία για ερευνητικούς σκοπούς (European Data Protection Supervisor, 2020). Θα πρέπει να γίνει έλεγχος συμβατότητας που μπορεί να εκτελεστεί, αν και εξ' αρχής η συμβατότητα σκοπών θα μπορούσε να θεωρηθεί δεδομένη για τους αρχικούς και για τους ακόλουθους ελεγκτές επεξεργασίας δεδομένων από την υγειονομική περίθαλψη για την επιστημονική έρευνα, όσο υπάρχουν οι κατάλληλες διασφαλίσεις. Αντίθετα, μια έρευνα της σουηδικής κυβέρνησης κατέληξε στο συμπέρασμα ότι ως προς τη συνέχιση της νομικής βάσης, μόνο η μεταβίβαση σε επόμενο υπεύθυνο επεξεργασίας καλύπτεται από την αρχική νομική βάση.

Ο νέος υπεύθυνος επεξεργασίας πρέπει να βρει τη δική του έγκυρη νομική βάση, αν θέλει να τα επεξεργαστεί. Το EDPB παραμένει σιωπηλό σχετικά με το θέμα αυτό στις κατευθυντήριες γραμμές του σχετικά με COVID-19 και έρευνα. Ωστόσο, ειδική καθοδήγηση αναμένεται για το θέμα της περαιτέρω επεξεργασίας (European Data Protection Supervisor, 2020). Δεδομένης της ασαφούς κατάστασης σχετικά με τη χρηστικότητα της προαναφερθείσας εξαίρεσης επεξεργασίας για την έρευνα, η θέσπιση νομικής βάσης με βάση το άρθρο 5 παράγραφος 1 στοιχείο β σε συνδυασμό με την αιτιολογική σκέψη 50 είναι αβέβαιη.

Νομιμοποίηση για την Επεξεργασία Ειδικών Κατηγοριών στα Δεδομένα (π.χ. Υγεία και Γενετικά δεδομένα)

Προσωπικά δεδομένα, που υποβάλλονται σε επεξεργασία για την έρευνα COVID-19, πάντα περιλαμβάνουν δεδομένα υγείας. Λαμβάνοντας υπόψιν ότι τα δεδομένα υγείας και γενετικής είναι «ειδικές κατηγορίες» δεδομένων σύμφωνα με το άρθρο 9, παράγραφος 1 του GDPR απαγορεύεται η επεξεργασία τους. Επομένως, τα ερευνητικά ιδρύματα χρειάζονται όχι μόνο μια νομική βάση, αλλά επίσης μια πρόσθετη νομιμοποίηση βάσει του άρθρου 9, παράγραφος 2 για την επεξεργασία των δεδομένων υγείας και γενετικής. Και πάλι, η συγκατάθεση είναι μια πιθανή επιλογή, ωστόσο αντιμετωπίζει πολλούς από τους περιορισμούς που περιγράφονται παραπάνω. Ο GDPR απαιτεί αυτή η συγκατάθεση να είναι τόσο ρητή όσο και συγκεκριμένη, όπως στην περίπτωση του άρθρου 9, παράγραφος 2 στοιχείο α.

Εφόσον η συγκατάθεση για έρευνα λαμβάνεται ρητά, η μεγαλύτερη πρόκληση εξακολουθεί να είναι η ερμηνεία του όρου "ειδικές". Ωστόσο, η αιτιολογική σκέψη 33 επιτρέπει τη συναίνεση για ευρύτερη έρευνα σε τομείς επιστημονικής έρευνας όπου οι λόγοι διεξαγωγής της δεν μπορούν να είναι πλήρως καθορισμένοι τη στιγμή που λαμβάνεται η συγκατάθεση. Εκεί όπου η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων, το EDBP ερμηνεύει περιοριστικά αυτή την άδεια (European Data Protection Board. Guidelines 05/2020, 2020). Αυτό μπορεί να θέσει προκλήσεις στην έρευνα για τον COVID-19, όπου χρειάζεται ένα μοντέλο ευρείας συναίνεσης, το οποίο μπορεί να καλύψει όλο το φάσμα της έρευνας (από μηχανισμούς νόσησης σε τρόπους μετάδοσης έως και σε ψυχολογικές ή κοινωνικοοικονομικές συνέπειες της νόσου). Έτσι, αυξάνονται τα καθήκοντα παροχής πληροφοριών του υπευθύνου επεξεργασίας

δεδομένων και δυσκολεύεται η καταγραφή και η συγκατάθεση (European Data Protection Board. Guidelines 05/2020, 2020). Είναι, συνεπώς, χρήσιμο να εξεταστούν άλλες επιλογές νομιμοποίησης.

Υπάρχουν δύο πιθανές επιλογές για την επεξεργασία δεδομένων υγείας και γενετικών δεδομένων για έρευνα στο πλαίσιο του COVID-19. Το άρθρο 9 παράγραφος 2 στοιχείο θ, που προβλέπει επεξεργασία για λόγους δημοσίου συμφέροντος στην περιοχή της δημόσιας υγείας, όπως η προστασία από σοβαρές διασυνοριακές απειλές για την υγεία. Επομένως, αυτό το άρθρο μπορεί να καλύψει την επεξεργασία στην περίπτωση μιας επιδημίας. Η νομοθεσία για τις λοιμώδεις νόσους και η έρευνα για μολυσματικές ασθένειες σε μια επιδημία μπορεί να είναι νόμιμες με βάση την παρούσα παράγραφο, αλλά μόνο εφόσον ο νόμος προβλέπει ρητή αναφορά σε έρευνα για τη δημόσια υγεία ή σε περίπτωση μιας επιδημίας. Το άρθρο 9, παράγραφος 2, στοιχείο ι, από την άλλη πλευρά, καλύπτει τυχόν επεξεργασία που είναι απαραίτητη για την επιστημονική έρευνα γενικά, ανεξάρτητα από το είδος της νόσου. Αυτή η νομιμοποίηση πρέπει επίσης να βασίζεται στο εκάστοτε δίκαιο της Ένωσης ή του κράτους μέλους.

Επιπλέον, απαιτούνται κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και συμφερόντων του υποκειμένου των δεδομένων. Ο GDPR είναι σιωπηλός σχετικά με το τι σημαίνει «κατάλληλα και συγκεκριμένα μέτρα για διασφάλιση» στο πλαίσιο αυτό. Ωστόσο, αυτά τα μέτρα πιθανότατα να συνδέονται με τις απαιτήσεις αναλογικότητας, ελαχιστοποίησης δεδομένων και ασφάλειας δεδομένων. Τα συγκεκριμένα μέτρα μπορεί να περιλαμβάνουν κρυπτογράφηση, ψευδωνυμοποίηση, ελαχιστοποίηση ευαίσθητων δεδομένων, που υποβάλλονται σε επεξεργασία, εκπαίδευση ειδικού

προσωπικού και επιβολή καθηκόντων εμπιστευτικότητας. Το συγκεντρωτικό αποτέλεσμα αυτών των μέτρων είναι η μείωση των κινδύνων επεξεργασίας ευαίσθητων προσωπικών δεδομένων (Georgieva L, Docksey C., 2021). Υπάρχει μεγάλη ετερογένεια μεταξύ των χωρών του ΕΟΧ ως προς το αν και πώς γίνεται χρήση αυτών των διατάξεων του GDPR. Για παράδειγμα, σχετικά με την εφαρμογή του άρθρου 9 παράγραφος 2 στοιχείο ι, το Ηνωμένο Βασίλειο (Data Protection Act 2018, 2018) και οι Κάτω Χώρες (Uitvoeringswet Algemene verordening gegevensbescherming, 2019) έχουν περιοριστεί στην εφαρμογή των διατάξεων αυτών στην έρευνα μόνο προς το δημόσιο συμφέρον, η Σουηδία απαιτεί έγκριση δεοντολογίας και η Φινλανδία έχει θέσει καθορισμένες απαιτήσεις για τεχνικές διασφαλίσεις (Tietosuojalaki, 2018).

Επιπλέον, ο GDPR δίνει εξουσίες στα κράτη μέλη να περάσουν πρόσθετους περιορισμούς στην επεξεργασία των δεδομένων υγείας και των γενετικών δεδομένων (άρθρο 9[4]), αυξάνοντας έτσι την πιθανότητα παρεκκλίσεων . Ορισμένες χώρες έχουν υιοθετήσει διαφορετικούς κανόνες για δεδομένα υγείας από τη μια και για γενετικά δεδομένα από την άλλη. Για παράδειγμα, η Ιρλανδία επανέφερε τη ρητή συναίνεση ως προαπαιτούμενο (χωρίς συγκεκριμένη κυβερνητική δήλωση σε κάποιες περιστάσεις) (Data Protection Act 2018, 2018). Ειδικά όταν χρησιμοποιούνται δεδομένα υγειονομικής περίθαλψης, πρέπει επίσης να λαμβάνονται υπόψιν οι κανόνες επαγγελματικού απορρήτου. Αυτές οι συνθήκες ακολουθούν την εθνική ή περιφερειακή νομοθεσία περί υγειονομικής περίθαλψης.

Κατά συνέπεια, έχει δημιουργηθεί ένα συγκεχυμένο συνονθύλευμα ετερογενών διατάξεων που αφορούν την επεξεργασία προσωπικών δεδομένων υγείας και γενετικών δεδομένων για μια έρευνα πανδημίας σε

όλη την Ευρώπη. Αυτή η μη αρμονική ποικιλία “διαφορετικών” λύσεων δεν είναι χρήσιμη εκεί όπου είναι απαραίτητη η παγκόσμια διασυνοριακή κοινή χρήση και απαιτούνται έγκαιρες λύσεις. Αυτό αποδεικνύεται επίσης από τις κατευθυντήριες γραμμές του EDPB για τον COVID-19 και την έρευνα (European Data Protection Board. Guidelines 03/2020, 2020). Οι συστάσεις παραμένουν σε ισχύ σε ένα γενικό επίπεδο και αναφέρονται σε λύσεις των κρατών μελών, χωρίς να συζητούνται περαιτέρω στο πλαίσιο και στις απαιτήσεις της πανδημίας. Για ένα πρόβλημα, που αντιμετωπίζει ομόφωνα η Ευρώπη, είμαστε δυστυχώς υποχρεωμένοι να επιστρέψουμε σε επίπεδο κρατών μελών για να βρεθούν λύσεις.

4.2 ΜΕΤΑΦΟΡΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΤΟΥ ΕΟΧ

Ενόψει μιας πραγματικά παγκόσμιας πανδημίας, υπάρχει σαφής ανάγκη οι ερευνητές να συνεργάζονται και να μοιράζονται γρήγορα και διεθνώς τα δεδομένα. Το Κεφάλαιο V του GDPR επιβάλλει περιορισμούς στη μεταφορά δεδομένων προσωπικού χαρακτήρα εκτός του ΕΟΧ, με στόχο να διασφαλιστεί ότι τα προσωπικά δεδομένα των Ευρωπαίων υπόκεινται σε ουσιαστικά ισοδύναμα επίπεδα προστασίας, όταν αποστέλλονται σε άλλες χώρες. Η απόφαση ισοδυναμίας των επιπέδων προστασίας, που χορηγείται από την Ευρωπαϊκή Επιτροπή, είναι η πιο απλή λύση που επιτρέπει την ανταλλαγή δεδομένων υπό τους ίδιους όρους, όπως εντός του ΕΟΧ (άρθρο 45).

Ωστόσο, σπάνια χορηγείται και μόνο δεκατρείς δικαιοδοσίες έχουν λάβει αναγνώριση (Adequacy decisions, 2021). Οι αποφάσεις περί ισοδυναμίας απαιτούν προσεκτική μελέτη, καθώς μερικές φορές καλύπτουν ορισμένους μόνο τομείς. Επιπλέον, η συνεχιζόμενη ισχύς των αποφάσεων ισοδυναμίας ενδέχεται να τεθεί σε κίνδυνο, εάν οι δικαιούχοι σε τρίτες χώρες υιοθετήσουν επιθετικές πρακτικές συλλογής και επεξεργασίας δεδομένων

σχετικών με τον COVID-19 (The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers, 2020; Wiewiórowski W., 2020).

Μια άλλη επιλογή είναι να υιοθετηθεί μία από τις κατάλληλες διασφαλίσεις για μεταβίβαση, που εισάγεται στο άρθρο 46. Η νομική δέσμευση και τα εκτελεστικά όργανα μπορεί να είναι μια ικανοποιητική διασφάλιση, ιδιαίτερα για την ανταλλαγή δεδομένων μεταξύ υγειονομικών αρχών (άρθρο 46[2][α]). Για την κοινή έρευνα, ωστόσο, υπάρχουν επί του παρόντος λίγα εκτελεστικά όργανα. Τα ιδρύματα μπορούν επίσης να βασίζονται στις τυπικές συμβατικές ρήτρες, που παρέχονται από την Ευρωπαϊκή Επιτροπή (άρθρο 46[2][γ]). Ένα αξιοσημείωτο πρόβλημα με αυτές τις ρήτρες, ωστόσο, είναι ότι τα κυβερνητικά τμήματα, τα δημόσια πανεπιστήμια και τα ακαδημαϊκά κέντρα υγείας των Η.Π.Α δεν μπορούν να συναινέσουν στην επίλυση διαφορών στα ευρωπαϊκά δικαστήρια (Peloquin D. Et al., 2020).

Εναλλακτικές συμβατικές ρήτρες ή διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών και φορέων θα απαιτείται να εγκριθούν από την αρχή προστασίας δεδομένων και δεν είναι πιθανό να παρέχουν ad hoc και γρήγορες λύσεις (άρθρο 46[3][α]). Η πανδημία, ωστόσο, μπορεί να δικαιολογήσει την εξάρτηση από παρεκκλίσεις για συγκεκριμένες καταστάσεις. Οι διασυνοριακές μεταφορές μπορούν να νομιμοποιηθούν με ρητή συγκατάθεση σύμφωνα με το άρθρο 49, παράγραφος 1 στοιχείο α, όμως τα ίδια πρακτικά εμπόδια θα πρέπει να ξεπεραστούν. Για παράδειγμα, το υποκείμενο των δεδομένων πρέπει να ενημερωθεί για τις συγκεκριμένες μεταγραφές που προβλέπονται, συνεπώς, δεν είναι δυνατό να δώσει ο κάτοχος των δεδομένων γενική συγκατάθεση για οποιεσδήποτε μελλοντικές, απροσδιόριστες μεταφορές εκτός του ΕΟΧ (Peloquin D. et al., 2018).

Το EDPB σημειώνει, επιπλέον, ότι η ρητή συγκατάθεση είναι απαραίτητη μόνο για ορισμένες περιπτώσεις, όπως για ιδιωτικούς φορείς που διεξάγουν έρευνες για τον COVID-19. Ωστόσο, εκτός από τις κατευθυντήριες οδηγίες για την έρευνα του COVID-19 δεν παρέχει περαιτέρω καθοδήγηση (παράγραφος 67). Μεταφορές δεδομένων απαραίτητες για σημαντικούς λόγους δημοσίου συμφέροντος, όπου αυτό το δημόσιο συμφέρον ορίζεται από το δίκαιο της Ένωσης ή το εθνικό δίκαιο (άρθρα 49[1][δ] και 49[4]), θα μπορούσαν να παρέχουν μια καταλληλότερη λύση στην αντιμετώπιση της πανδημίας, ιδίως λόγω της διασυνοριακής συνεργατικής έρευνας, που είναι μια σημαντική πτυχή για την καταπολέμησή της.

Ωστόσο, το EDPB προειδοποιεί επίσης ότι μεταφορές σύμφωνα με αυτό το άρθρο «δεν θα γίνονται συχνά», θα περιορίζονται σε «συγκεκριμένες καταστάσεις» και θα είναι «μόνο οι αυστηρά απαραίτητες» για τους σκοπούς της επεξεργασίας. Στη συγκεκριμένη περίσταση του ξεσπάσματος του COVID-19, το EDPB παραδέχτηκε «ότι ο αγώνας κατά του COVID-19 έχει αναγνωριστεί από την Ε.Ε. και τα περισσότερα κράτη μέλη του ως σημαντικό δημόσιο συμφέρον», στηρίζοντας αυτόν τον ισχυρισμό του στο ότι διατάξεις του δικαίου της Ε.Ε. ερμηνεύτηκαν υπό το πρίσμα της κρίσης και έτσι πρακτικά τροποποιήθηκαν από τα κράτη μέλη (παράγραφοι 62-67).

Ο χρόνος θα δείξει ότι οι διεθνείς μεταφορές δεδομένων με βάση το δημόσιο συμφέρον θα είναι μια αποδεκτή λύση σε όλη την Ευρώπη. Οι ερευνητές, που δεν ενεργούν υπό την αιγίδα δημόσιας αρχής, επομένως καμία από αυτές τις επιλογές δεν μπορεί να εφαρμοστεί στην περίπτωσή τους, μπορούν τουλάχιστον να ισχυριστούν ως άμεσο μέτρο ότι η μεταφορά δεδομένων είναι απαραίτητη για λόγους επιτακτικού, νόμιμου συμφέροντος, που δεν καταπατά τα συμφέροντα ή τα δικαιώματα και τις

ελευθερίες του υποκειμένου των δεδομένων (άρθρο 49[1]). Τέτοιες μεταφορές υπόκεινται σε μυριάδες περιορισμούς, για παράδειγμα, η μεταφορά πρέπει να μην είναι επαναλαμβανόμενη, να αφορά μόνο περιορισμένο αριθμό υποκειμένων δεδομένων, να εφαρμόζονται κατάλληλες ασφάλειες και τέλος να υποστηρίζεται με αποδείξεις στην αρμόδια αρχή προστασίας δεδομένων ότι δεν υπάρχει άλλη διαθέσιμη επιλογή (άρθρο 49[1]). Αυτό είναι, στην καλύτερη περίπτωση, μια ενδιάμεση λύση. Το EDPB αναγνωρίζει τη σημασία των διεθνών μεταφορών για πανδημική έρευνα, αν και ίσως με μισή καρδιά μόνο («πιθανώς» απαιτούνται μεταφορές) (European Data Protection Board. Guidelines 03/2020, 2020). Το EDPB προτείνει επίσης ότι οι υφιστάμενες διατάξεις βάσει του GDPR επαρκούν για την πραγματοποίηση τέτοιων μεταφορών. Δεδομένου ότι στην ευρωπαϊκή έρευνα η κοινότητα εξακολουθεί να περιμένει λύσεις για διεθνή έρευνα και κοινή χρήση δεδομένων, που θα αναπτύσσονται και εκτός του πλαισίου της πανδημίας, η έλλειψη σαφούς λύσης παραμένει μια σοβαρή ανησυχία.

Ένα επιπλέον εμπόδιο δημιουργείται από την αυστηρή υποχρέωση παροχής πληροφοριών που έχουν τα ερευνητικά ιδρύματα απέναντι στους κατόχους των δεδομένων βάσει του GDPR. Εκτενείς πληροφορίες σχετικά με τη χρήση δεδομένων πρέπει να παρέχονται στο υποκείμενο των δεδομένων πριν τη συλλογή, συμπεριλαμβανομένων των πληροφοριών σχετικά με τη νομική βάση για την επεξεργασία τους και την πρόθεση μεταφοράς προσωπικών δεδομένων σε τρίτες χώρες (άρθρο 13). Υπάρχουν μόνο λεπτές εξαιρέσεις στην απαίτηση να παρέχονται άμεσα πληροφορίες στο υποκείμενο των δεδομένων. Εξαιρέσεις προβλέπονται σε περιπτώσεις που δεν λαμβάνονται δεδομένα απευθείας από το υποκείμενο των δεδομένων (άρθρο 14).

Έρευνα για τον COVID-19 που απαιτεί δευτερογενή χρήση δεδομένων, τα οποία έχουν συλλεχθεί κατά τη διάρκεια της φροντίδας των σοβαρά αρρώστων ασθενών μπορεί να εμπίπτουν σε αυτήν την εξαίρεση. Εκεί όπου η ενημέρωση περί του αντικειμένου μιας τέτοιας έρευνας θα ήταν αδύνατη ή θα απαιτούσε δυσανάλογη προσπάθεια, οι γενικές πληροφορίες μπορεί να κοινοποιούνται στην ιστοσελίδα του αρμόδιου ελεγκτή ή στις δημόσιες ανακοινώσεις. Η έρευνα πρέπει να υπόκειται στις κατάλληλες διασφαλίσεις που περιγράφονται στο άρθρο 89. Ωστόσο, ακόμα και για την περίπτωση της δευτερογενούς χρήσης των δεδομένων, που συλλέγονται κατά την υγειονομική περίθαλψη, ο αρχικός ελεγκτής (δηλαδή ο πάροχος υγειονομικής περίθαλψης) θα εξακολουθεί να είναι υποχρεωμένος να ενημερώσει το υποκείμενο των δεδομένων σχετικά με την κοινή τους χρήση για περαιτέρω επεξεργασία στο ερευνητικό πλαίσιο. Τα προβλήματα της εφαρμογής αυτών των απαιτήσεων είναι τα ίδια με παραπάνω: παροχή πρόσθετων πληροφοριών στο κλινικό πλαίσιο κατά τη διάρκεια έκτακτης ανάγκης, με πολλούς ασθενείς σε μια σοβαρή κατάσταση ασθένειας και προβλήματα αναπνοής, μπορεί να μην είναι εφικτή.

Δεδομένου ότι δεν προβλέπεται παρέκκλιση, δεν είναι σαφές το πώς οι αρχές προστασίας δεδομένων θα κρίνουν τυχόν αναδρομικές πληροφορίες που παρέχονται στους ασθενείς που επιβιώνουν από τη νόσο τους. Μια διέξοδος θα μπορούσε να βασίζεται σε διατάξεις που επιτρέπουν τον περιορισμό των δικαιωμάτων όλων των υποκειμένων των δεδομένων σε θέματα σημαντικού δημόσιου ενδιαφέροντος, όπως η δημόσια υγεία (άρθρο 23). Και πάλι, εθνικοί ή ευρωπαϊκοί νόμοι θα πρέπει να παρέχουν το απαραίτητο πλαίσιο αναφοράς.

Μόνο λίγα κράτη μέλη έχουν εφαρμόσει τέτοιου είδους παρεκκλίσεις στην εθνική νομοθεσία για την προστασία δεδομένων, και συχνά είναι

επιφανειακές, αναφέροντας τη δυνατότητα παρεκκλίσεων για τη δημόσια υγεία, μεταξύ άλλων (Uitvoeringswet Algemene verordening gegevensbescherming, 2019 & the Data Protection Act, 2018). Δεν υπάρχουν λεπτομερείς διατάξεις ειδικά για σχετικές ερευνητικές πτυχές για τη διατήρηση της δημόσιας υγείας. Η προκύπτουσα νομική αβεβαιότητα εμποδίζει την ανταποκρινόμενη έρευνα κατά τη διάρκεια μιας πανδημίας, εάν δεν είναι εφικτή η παροχή απαραίτητων πληροφοριών πριν από την έναρξη της έρευνας.

4.3 ΕΦΑΡΜΟΖΟΜΕΝΟΙ ΚΑΝΟΝΙΣΜΟΙ ΣΕ ΠΕΡΙΠΤΩΣΕΙΣ ΚΑΤΑΣΤΑΣΕΩΝ ΕΚΤΑΚΤΗΣ ΑΝΑΓΚΗΣ

Πολλές χώρες του ΕΟΧ προβλέπουν τη δυνατότητα της κυβέρνησης σε καταστάσεις έκτακτης ανάγκης να θεσπίζει νόμους για να αντιμετωπίσει μια κρίση, όπως μια πανδημία. Οι διατάξεις αυτές μπορούν να περιορίσουν τα δικαιώματα των πολιτών, συμπεριλαμβανομένης της προστασίας των δικαιωμάτων των δεδομένων τους, όπως προβλέπονται στον ίδιο τον GDPR (άρθρο 23).

Σε μία πανδημία, τέτοιοι κανονισμοί μπορούν να παρεκκλίνουν από τα δικαιώματα των υποκειμένων των δεδομένων και να παρέχουν μια νομική βάση για επεξεργασία πέραν του υφιστάμενου νομικού πλαισίου. Αυτές οι εξουσίες έκτακτης ανάγκης δεν ισοδυναμούν με λευκή κάρτα, τα μέτρα πρέπει να είναι απαραίτητα, κατάλληλα και ανάλογα με τον επιδιωκόμενο στόχο. Το EDPB επισημαίνει, επίσης, ότι τα μέτρα που εφαρμόζονται βάσει έκτακτης ανάγκης, πρέπει να περιορίζονται αυστηρά και μόνο στη διάρκεια της έκτακτης ανάγκης (European Data Protection Board, 2020). Επιπλέον, για να βασίζονται εύλογα σε τέτοιες εξουσίες , θα πρέπει να υπάρχει μια στενή σύνδεση μεταξύ της έρευνας, που διεξήχθη, και της αντιμετώπισης της πανδημίας.

Τέτοια μέτρα υπόκεινται επίσης σε επίβλεψη από εθνικά συνταγματικά ή διοικητικά δικαστήρια, καθώς και το Δικαστήριο της Ευρωπαϊκής Ένωσης και το Ευρωπαϊκό Δικαστήριο για τα Ανθρώπινα δικαιώματα. Συζητήσεις, σχετικά με τις έκτακτες παρεκκλίσεις στο πλαίσιο της επεξεργασίας των δεδομένων, έχουν επικεντρωθεί μέχρι στιγμής σε μεγάλο βαθμό στην παρακολούθηση τοποθεσίας ή ανίχνευση επαφής μεταξύ κρουσμάτων και άλλων ατόμων με τη χρήση κινητών τηλεφώνων και όχι στην έρευνα για την υγεία. Τέτοια μέτρα μπορούν να χρησιμοποιηθούν για την αναγνώριση ατόμων σε κίνδυνο και την παρακολούθηση της τήρησης της κοινωνικής απόστασης. Το EDPB έχει εκδώσει επιστολή προς την Ευρωπαϊκή Επιτροπή δηλώνοντας ότι η θέσπιση εθνικών νόμων θα ήταν ένας καλός τρόπος για την παροχή ενός στέρεου νομικού πλαισίου για τον καθορισμό του πεδίου εφαρμογής και, επίσης, του περιορισμού της διάρκειας της οποιασδήποτε χρήσης πληροφοριών από κινητά τηλέφωνα, ακολουθούμενη από απενεργοποίηση των συστημάτων παρακολούθησης και διαγραφή των δεδομένων μόλις τελειώσει η κρίση (European Data Protection Board, 2020).

Παράλληλα, το EDPB επιμένει ότι η χρήση μιας εφαρμογής θα μπορούσε να είναι εθελοντική και να μην γίνεται υποχρεωτικό μέτρο ή να εμπεριέχει τυχόν μειονεκτήματα για όσους δεν επιλέγουν τη χρήση της. Τα δικαιώματα των υποκειμένων των δεδομένων δεν πρέπει να υπόκεινται σε συμβιβασμούς, αλλά θα πρέπει αντιθέτως να παραμείνουν σεβαστά για να διατηρηθεί η εμπιστοσύνη των πολιτών. Στο ίδιο πνεύμα, μια κοινή δήλωση έχει υπογραφεί από περισσότερους από 550 ερευνητές σε όλο τον κόσμο κάνοντας έκκληση για διατήρηση της ιδιωτικής ζωής, αυστηρό περιορισμό τέτοιων τεχνολογιών για σκοπούς σχετικούς με τον COVID-19 και αυστηρά εθελοντική βάση για τη χρήση οποιασδήποτε εφαρμογής ανίχνευσης επαφών (Contact Tracing Joint Statement, 2020).

Το θέμα της χρήσης των τεχνολογιών ανίχνευσης επαφών συνδέεται με τη συλλογή στοιχείων, που βοηθούν την έρευνα (που αναφέραμε πιο πάνω) π.χ. πληροφορίες που συλλέγονται ως μέρος της παρακολούθησης και της ανίχνευσης επαφών θα μπορούσαν να υποστηρίξουν την έρευνα στη μελέτη της πορείας της πανδημίας και τους μηχανισμούς μετάδοσης του ιού. Παράδειγμα έκτακτης νομοθεσίας με συγκεκριμένες διατάξεις για έρευνα εισήχθη στην Ιταλία, όπου η υποχρέωση που υπήρχε για διαβούλευση με την αρχή προστασίας δεδομένων, σε περιπτώσεις που συγκατάθεση δεν ήταν εφικτό να ληφθεί, μπορεί να αίρεται σε ορισμένες περιστάσεις (Garante per la protezione dei dati personali, 2020).

Αυτή η απαίτηση ήταν υπερβολική ακόμη και σε κανονικές συνθήκες. Ωστόσο, στην παρούσα κατάσταση της κρίσης COVID-19, ισχύει μόνο σε κλινικές δοκιμές και μελέτες παρατήρησης φαρμακευτικών προϊόντων, που είναι απαραίτητες για την καταπολέμηση της νόσου καθώς και για τα ερευνητικά προγράμματα COVID-19, που χρηματοδοτούνται από τα Ινστιτούτα Επιστημονικής Νοσηλείας και Θεραπείας και το Υπουργείο Υγείας. Επίσης, παρεκκλίσεις από το άρθρο 13 του GDPR έχουν γίνει με βάση το άρθρο 23, παράγραφος 1 στοιχείο ε. Η ιταλική άρση των δικαιωμάτων δείχνει πώς η τρέχουσα πανδημία εκθέτει τις αδυναμίες της νομοθεσίας για την προστασία δεδομένων και την έρευνα και πώς οι κανονισμοί έκτακτης ανάγκης μπορούν να χρησιμοποιηθούν ως μια γρήγορη, αν και προσωρινή θεραπεία.

ΚΕΦΑΛΑΙΟ 5: GDPR ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ

Ο GDPR αναφέρει πως οι οργανισμοί οφείλουν να καταστήσουν τις αρχές προστασίας δεδομένων εγγενή μέρη των εσωτερικών μέτρων και λειτουργιών τους. Απαιτεί να εφαρμόσουν κατάλληλες τεχνικές, τόσο τεχνολογικές όσο και λειτουργικές για την εξασφάλιση των προσωπικών δεδομένων.

5.1 Η ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR ΣΤΟΝ ΤΟΜΕΑ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Ο GDPR έχει αντικαταστήσει την οδηγία του 1995, η οποία, μεταξύ άλλων, διέφερε έντονα στην εφαρμογή της από τη μια χώρα στην άλλη και συντάχθηκε με τα δεδομένα μιας εποχής, όπου το διαδίκτυο δεν ήταν ευρέως διαδεδομένο. Ο GDPR δεν είναι ρυθμιστικός, δηλαδή δεν απαιτεί τη χρήση συγκεκριμένης τεχνολογίας για την επίτευξη του στόχου, προς αποφυγήν του κινδύνου να απαρχαιωθεί σύντομα, καθώς ο γοργός ρυθμός ανάπτυξης της τεχνολογίας σημαίνει πως η σημερινή κορυφαία τεχνολογία μπορεί να αντικατασταθεί πλήρως από μια άλλη ακόμα και σε χρονικό διάστημα μηνών, σε κάποιες ακραίες περιπτώσεις. Είναι άλλωστε συνηθισμένο να δίνεται μια σχετική ελευθερία όσον αφορά τα μέσα που θα αξιοποιηθούν για την εφαρμογή νέων νομοθεσιών, κάτι που ισχύει ακόμα περισσότερο στον τομέα της τεχνολογίας (Colin Tankard,2016).

Έτσι, ο κανονισμός απαιτεί από τους οργανισμούς να εφαρμόσουν κατάλληλες τεχνικές, τόσο τεχνολογικές όσο και λειτουργικές για την εξασφάλιση των δεδομένων. Μεταξύ αυτών συμπεριλαμβάνεται η δημιουργία και εφαρμογή ισχυρών ελέγχων της ιδιωτικότητας. Ο κανονισμός αναφέρει πως οι οργανισμοί οφείλουν να κάνουν τις αρχές προστασίας δεδομένων εγγενή μέρη των εσωτερικών μέτρων και λειτουργιών τους. Ουσιαστικά, το ζητούμενο είναι η ασφάλεια των

δεδομένων και η ιδιωτικότητα να αντιμετωπίζονται ως κύριο μέλημα και όχι ως δεύτερο κατά τη διαδικασία σχεδίασης της ασφάλειας.

Υπάρχει, ωστόσο, μια εξαίρεση στον κατά τα άλλα μη ρυθμιστικό αυτόν κανονισμό. Η κρυπτογράφηση και η δυνατότητα χρήσης ψευδώνυμου, η ψευδωνυμοποίηση, αναφέρονται εκπεφρασμένα ως κατάλληλες μέθοδοι διασφάλισης των δεδομένων. Εφόσον αυτές έχουν εφαρμοστεί ορθά, οι οργανισμοί των οποίων τα δεδομένα παραβιάζονται δεν θα οφείλουν να ειδοποιήσουν τους ιδιοκτήτες των δεδομένων, καθώς τα δεδομένα θεωρούνται επαρκώς προστατευμένα. Στην περίπτωση της ψευδωνυμοποίησης συγκεκριμένα, όταν αυτή έχει γίνει με τέτοιον τρόπο ώστε τα δεδομένα να είναι αδύνατον να αποδοθούν σε συγκεκριμένο άτομο ή χρήστη, τότε αυτά τα δεδομένα πρέπει να φυλάσσονται ξεχωριστά από άλλες πληροφορίες προς διασφάλιση της ανωνυμίας του κατόχου. Η κρυπτογράφηση είναι η κύρια τεχνολογία που χρησιμοποιείται για την προστασία των δεδομένων.

Όπως αναφέρθηκε και προηγουμένως, η κρυπτογράφηση είναι μια από τις δυο τεχνολογίες που ο κανονισμός ονομάζει και θεωρεί πως θα πρέπει να είναι η προεπιλεγμένη μέθοδος για την προστασία δεδομένων, είτε αυτά μεταφέρονται, είτε είναι αποθηκευμένα. Αυτό συμπεριλαμβάνει τόσο δομημένα όσο και μη δομημένα δεδομένα που είναι αποθηκευμένα σε βάσεις δεδομένων ή εντός εγγράφων και μηνύματα ηλεκτρονικού ταχυδρομείου. Ακόμα και όταν τα δεδομένα είναι αποθηκευμένα στο «cloud» ή σε τερματικά σημεία, κρυπτογραφικά κλειδιά, πρέπει να φυλάσσονται από τον υπεύθυνο του οργανισμού για τη συλλογή και επεξεργασία των δεδομένων, προς αποφυγήν περιπτώσεων που κάποιος τρίτος θα προσπαθούσε να αποκτήσει παράνομη πρόσβαση στα δεδομένα. Σε τέτοια περίπτωση, θα μπορούσαν να υπάρξουν κατηγορίες σε βάρος του

οργανισμού στηριζόμενες στο ότι η κρυπτογράφηση δεν εφαρμόστηκε επαρκώς ή ορθά. Μέτρα προστασίας πρέπει να υπάρχουν και εντός του οργανισμού για να εξασφαλίσουν πως μόνο τα άτομα που χειρίζονται τα κλειδιά θα έχουν πρόσβαση σε αυτά.

Παρότι τα δεδομένα κρυπτογραφούνται, βοηθάει να ελαχιστοποιείται ο όγκος των δεδομένων που συλλέγεται. Αυτό δεν θα μειώσει μόνο το βάρος που ενυπάρχει στην προστασία μεγάλων βάσεων δεδομένων, αλλά θα μειώσει και την πιθανότητα ο οργανισμός να παραβεί την προϋπόθεση του κανονισμού ότι τα δεδομένα πρέπει να χρησιμοποιούνται μόνο για τον σκοπό για τον οποίο συλλέχθηκαν και κανέναν άλλον. Αν γίνει χρήση των δεδομένων πέραν αυτών στις οποίες ο ιδιοκτήτης τους συμφώνησε, θα δικαιούται να ζητήσει οικονομική αποζημίωση (Colin Tankard, 2016).

Ενώ λοιπόν η κρυπτογράφηση είναι ένα εξαιρετικά χρήσιμο εργαλείο όσον αφορά την προστασία δεδομένων, δεν είναι επαρκές από μόνο του. Οι οργανισμοί οφείλουν να βεβαιωθούν πως έχουν κατάλληλα μέτρα για πρόσβαση σε έλεγχο, για να αποτρέψουν περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε κρυπτογραφημένα δεδομένα και να ελέγχουν τι μπορεί να κάνει ο κάθε χρήστης με τα δεδομένα σύμφωνα με τον ρόλο του. Έτσι, ένας διαχειριστής συστήματος πρέπει να είναι σε θέση να εκπληρώσει τα διοικητικά του καθήκοντα χωρίς όμως να μπορεί να διαβάσει το περιεχόμενο των δεδομένων. Για παράδειγμα, σε ένα σύστημα διαχείρισης ανθρώπινων πόρων, οι τεχνικοί χρειάζεται να ξέρουν πως τα δεδομένα είναι εκεί που περιμένουν, αλλά να μην μπορούν να διαβάσουν τα συμβόλαια εργασίας. Αυτό ισχύει, κατά τον ίδιο τρόπο, σε εφαρμογές που έχουν πρόσβαση σε δεδομένα και στις οποίες θα πρέπει να επιβληθεί έλεγχος πρόσβασης.

Για αυτόν τον λόγο, οι έλεγχοι θα πρέπει να συνδέονται με βάσεις δεδομένων που λειτουργούν στο παρασκήνιο, όπως για παράδειγμα τον Ενεργό Κατάλογο (Active Directory), κάτι που θα βοηθήσει στον προσδιορισμό αναλυτικών δικαιωμάτων και θα εξασφαλίσει πως οι έλεγχοι είναι ενημερωμένοι καθώς τα πράγματα αλλάζουν, όπως στην περίπτωση που κάποιος προάγεται ή μετατίθεται.

Εάν, ωστόσο, κάποιος οργανισμός βρίσκει πως η διαχείριση του Ενεργού Καταλόγου είναι υπερβολικά περίπλοκη, μπορεί να κάνει χρήση εργαλείων, τα οποία διατίθενται από εταιρείες ανάπτυξης λογισμικού και επιτρέπουν σε μια επιχείρηση να έχει εικόνα σε μορφή γραφήματος των δικαιωμάτων των χρηστών της και να αφαιρεί ή να προσθέτει σημεία ελέγχου προς διευκόλυνση της διαχείρισης χρηστών. Επιπλέον, η σύνδεση της ταυτοποίησης χρηστών ή εφαρμογών με την κρυπτογράφηση ενισχύει τα διαθέσιμα εργαλεία ελέγχου που είναι διαθέσιμα εντός του Ενεργού Καταλόγου και προσφέρει αναλυτική διαδρομή ελέγχου (audit trail) των χρηστών, κάτι που ενισχύει την ικανότητα παρακολούθησης και καταγραφής εσωτερικών απειλών, τις οποίες πολλοί οργανισμοί αντιμετωπίζουν. Η χρήση ισχυρού ελέγχου ταυτότητας θα βοηθήσει για να διασφαλιστεί ότι τα άτομα που έχουν πρόσβαση στα δεδομένα είναι αυτά που δηλώνουν, έτσι ώστε ένας χρήστης με δικαιώματα πρόσβασης σε συγκεκριμένα δεδομένα να μην μπορεί να τα μεταβιβάσει σε κάποιον άλλο (Colin Tankard, 2016).

Για να ελεγχθεί και να αξιολογηθεί ότι οι έλεγχοι είναι αποτελεσματικοί και να διασφαλιστεί ότι λειτουργούν ανά πάσα στιγμή, όλα τα συστήματα ασφάλειας θα πρέπει να παρακολουθούνται συνεχώς, λαμβάνοντας υπόψη όλους τους κινδύνους που σχετίζονται με την επεξεργασία και την αποθήκευση δεδομένων ηλικίας, συμπεριλαμβανομένης της ακούσιας

απώλειας ή καταστροφής. Ενσωμάτωση με πληροφορίες ασφαλείας και συστήματα διαχείρισης εκδηλώσεων και συμβάντων παρέχουν διαφάνεια σε συμβάντα μέσω του δικτύου, τα οποία μπορούν να αναλυθούν για να επιβεβαιωθεί πως οι στόχοι της ασφάλειας και συμμόρφωσης επιτυγχάνονται. Αυτό επίσης θα παρέχει τη διαδρομή ελέγχου που απαιτείται για να αποδειχτεί ότι οι έλεγχοι λειτουργούν σωστά.

Η χρήση των βιομηχανικών προτύπων και των βέλτιστων πρακτικών πλαισίων μπορούν να βοηθήσουν τις οργανώσεις στη διαχείριση των κινδύνων, που αντιμετωπίζουν, ενώ αυξάνουν την αποτελεσματικότητα και τη βιωσιμότητα των λειτουργιών τους και επιτρέπουν έτσι τις βέλτιστες πρακτικές να ενσωματωθούν στον οργανισμό.

Οι κρίσιμοι έλεγχοι ασφαλείας του CIS (Center of Internet Security), μπορούν να θεωρηθούν ως μια λίστα ελέγχων που οι οργανισμοί θα πρέπει να εφαρμόσουν για να είναι βέβαιοι πως το σύστημα ασφαλείας τους είναι ικανό να διαχειριστεί τον κίνδυνο. Αυτοί οι έλεγχοι είναι ένα προτεινόμενο σύνολο ενεργειών που παρέχουν στους οργανισμούς συγκεκριμένους και δραστικούς τρόπους για την ενίσχυση των δυνατοτήτων της κυβερνοασφάλειάς τους, επιτρέποντάς τους να δώσουν προτεραιότητα σε ενεργές δράσεις καταπολέμησης, σε περίπτωση επίθεσης, προκειμένου να επιτευχθούν τα καλύτερα αποτελέσματα με την ελάχιστη προσπάθεια.

Πρότυπα ασφάλειας όπως το ISO 27001 και το ISO 27002 βοηθούν τους οργανισμούς να διασφαλίσουν ότι έχουν εφαρμόσει αποτελεσματικά προγράμματα ασφάλειας. Το ISO 27001 δημιουργήθηκε αρχικά με την πρόθεση να βοηθήσει στη διαχείριση της ασφάλειας των κρατικών υπηρεσιών και των δεδομένων πολιτών, που βρίσκονταν στα χέρια των διαφόρων παρόχων υπηρεσιών. Η χρήση του ISO 27001 βοηθάει στη διασφάλιση της αρχής, που κατοχυρώνεται στον GDPR, ότι κατάλληλα

τεχνολογικά και οργανωτικά μέτρα υπάρχουν για την προστασία των πληροφοριών. Υποστηρίζει τους οργανισμούς στην προσπάθειά τους να καθορίσουν ευθύνες, όπως ποιος είναι υπεύθυνος για ορισμένες πληροφορίες και ποιος μπορεί να εξουσιοδοτήσει την πρόσβαση στα δεδομένα. Το ISO 27001 παρέχει ανεξάρτητη διαπίστευση για συστήματα διαχείρισης ασφάλειας πληροφοριών, ενώ το ISO 27002 είναι κώδικας πρακτικής που δεν είναι πιστοποιημένος από εξωτερικούς φορείς. Η χρήση οποιουδήποτε εξ αυτών θα βοηθήσει να φανεί ότι η οργάνωση έχει θέσει σε εφαρμογή αυστηρούς ελέγχους, αν ο οργανισμός βρεθεί αντιμέτωπος με ζητήματα που σχετίζονται με αμέλεια (Colin Tankard, 2016).

5.2 Ο ΑΝΤΙΚΤΥΠΟΣ ΤΟΥ GDPR ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Όπως αναφέρθηκε παραπάνω, ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) έχει σκοπό να προστατεύει το απόρρητο των δεδομένων των πολιτών της Ε.Ε. Τα οφέλη του κανονισμού για τα δικαιώματα των καταναλωτών και η ισχύς που δίνει στις ρυθμιστικές αρχές είναι ευρέως γνωστά, τα οφέλη για τις επιχειρήσεις όχι και τόσο.

Σε αυτή την παράγραφο θα μελετήσουμε ποια είναι τα οφέλη, αν υπάρχουν, του GDPR για τις επιχειρήσεις. Έχει παρατηρηθεί ότι υπό την απειλή των προστίμων του GDPR το επιχειρηματικό «δαιμόνιο» δραστηριοποιήθηκε, με αποτέλεσμα να ληφθούν τα ακόλουθα μέτρα για την προστασία της ιδιωτικότητας; αρχικά έχουν αλλάξει δομή οι εταιρείες τοποθετώντας ικανά στελέχη στον έλεγχο εφαρμογής του GDPR. Έχουν εκσυγχρονίσει τις διαδικτυακές πλατφόρμες, κάτι που τις βοηθά έμμεσα να γίνουν αποτελεσματικότερες στην αντιμετώπιση κινδύνων, όπως η διαρροή πληροφοριών και οι βάσεις δεδομένων των πελατών τους έχουν γίνει πιο ασφαλείς και ενημερωμένες. Επιπλέον, η συμμόρφωση χρησιμοποιείται

από κάποιους και για διαφημιστικούς λόγους, ως σήμα αξιοπιστίας. Από την άλλη πλευρά, διαπιστώνουμε ότι πολλές προκλήσεις παραμένουν προς εφαρμογή. Η ανάπτυξη των νέων επιχειρήσεων είναι δύσκολη και οι ενδοεπιχειρησιακές επικοινωνίες περιορισμένες. Έχει αυξηθεί το κόστος και η εσωτερική γραφειοκρατία. Επιπλέον, παραμένουν γκρίζες ζώνες λόγω ελλείψεων στις τροπολογίες. Ένα άλλο πρόβλημα είναι ότι οι πρώην υπάλληλοι ή δυσαρεστημένοι πελάτες εκμεταλλεύονται τα SAR (subject access requests) και τα χρησιμοποιούν ως μέσο για εκδίκηση. Οι μικρές επιχειρήσεις θεωρούν τον GDPR ως υπερβολικό και συντριπτικό. Συμπεραίνουμε ότι μολονότι ο GDPR μπορεί να θεωρηθεί επίπονος για τις επιχειρήσεις, εντούτοις τους έχει επιστήσει την προσοχή στη διαχείριση των δεδομένων.

Πολλοί πιστεύουν ότι αξίζει η Ε.Ε. να εξετάσει το ενδεχόμενο προσαρμογής μίας έκδοσης του κανονισμού για να ταιριάζει καλύτερα στις μικρομεσαίες επιχειρήσεις και να τροποποιήσει τον τρόπο γραφής του, ώστε να είναι πιο θετικός, ενώ θα εξακολουθεί να χρησιμοποιεί την απειλή των προστίμων για να ενισχύσει την πειθαρχία των εταιρειών στη διαχείριση των δεδομένων.

Ο κόσμος ανέκαθεν αντιμετώπιζε τη νομοθεσία ως κάτι βαρετό, γραφειοκρατικό και περιττό. Σε έναν βαθμό αυτά ισχύουν, αλλά είναι και ζωτικό εργαλείο της κυβέρνησης στην προσπάθειά εφαρμογής των πολιτικών της. Οι κυβερνήσεις νομοθετούν σχετικά με τις επιχειρήσεις, για να προσφέρουν καλύτερα αποτελέσματα στην οικονομία, το περιβάλλον και την κοινωνία. Για παράδειγμα, με νόμους ρυθμίζονται η διόρθωση προβλημάτων στη αγορά, η προστασία του ανθρώπου και της άγριας φύσης από τη ρύπανση και η ιδιωτική προστασία των πολιτών. Ο GDPR της Ε.Ε. είναι ένα καλό παράδειγμα του τελευταίου.

Σε αυτή την παράγραφο θα κάνουμε μια ανασκόπηση ήδη υπαρχουσών ερευνών και θα μελετήσουμε την επιρροή του GDPR στις επιχειρήσεις, κάτι που δεν έχει μελετηθεί ιδιαίτερα, παρόλο που αυτές θα επωμιστούν το κόστος της εφαρμογής του. Πρόσφατες ακαδημαϊκές έρευνες υπέθεταν ότι τα οφέλη του GDPR για τις επιχειρήσεις θα ήταν οι καλύτερες βάσεις δεδομένων, καλύτερες αναλύσεις των πελατών, βελτίωση της δημόσιας εικόνας της εταιρείας και ισότητα ανταγωνισμού.

Οι δυσκολίες του GDPR για τις επιχειρήσεις είναι γνωστές. Αρχικά, η συμμόρφωση μπορεί να είναι ακριβή (Maria Addis and Maria Kutar, 2018 & Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, 2018). Οι εταιρείες μπορεί να χρειάζονται επιπλέον διοικητικό και εξειδικευμένο προσωπικό DPO (Peter Lindgren, 2016), επιπλέον εκπαίδευση εργαζομένων ενώ, την ίδια στιγμή, αντιμετωπίζουν δυσκολίες στην πρόσληψη και στη διατήρηση αυτών των ατόμων (Javid Khan, 2018). Οι περιορισμοί που θέτει ο GDPR μπορεί να επηρεάσουν την απόδοση ενός οργανισμού (Erik van der Marel, Matthias Bauer, Hosuk LeeMakiyama and Bert Verschelde, 2016:12-39) και να πείσουν ορισμένες εταιρείες να μειώσουν την προσφορά υπηρεσιών τους στην Ε.Ε. για να τον αποφύγουν (Darcy W. E. Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler and Jason Potts, 2019). Ο GDPR έχει φέρει αυξημένη τεχνική πολυπλοκότητα (Colin J. Bennett, 2018 & Daria Dubrova, 2018 & Eugenia Politou, Efthimios Alepis and Constantinos Patsakis, 2018). Η δυνατότητα μεταφοράς δεδομένων (Wang Kaushik,2018), καθώς και οι διαδικασίες συναίνεσης, διόρθωσης και διαγραφής δεδομένων απαιτούν επένδυση σε τεχνικές και οργανωτικές τεχνικές από τις εταιρείες (Daria Dubrova, 2018). Η διαγραφή δεδομένων (γνωστή και ως δικαίωμα στη λήθη) θεωρείται ιδιαίτερα προβληματική για τις μεγάλες εταιρείες (Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay and Ignacio Sanchez, 2018 & Edward S. Dove,

2018). Οι έλεγχοι συστημάτων και διαδικασιών (Daria Dubrova, 2018) και η πρόσληψη περισσότερων επαγγελματιών στον τομέα της κυβερνοασφάλειας καταναλώνουν διαθέσιμους πόρους της εταιρείας. Οι περιορισμοί στον τρόπο χειρισμού των προσωπικών δεδομένων μπορούν να επιβαρύνουν την ανάπτυξη και την εφαρμογή αναδυόμενων τεχνολογιών όπως oIot και blockchain (He Li, Lu Yu, and Wu He,2018:1-6 & Nick Wallace and Daniel Castro, 2018).

Μελέτη των επιτυχιών του GDPR σε σχέση με τις επιχειρήσεις

Η αξιολόγηση του GDPR από την Oxford Analytica, ανεξάρτητη εταιρεία γεωπολιτικής ανάλυσης (Oxford Analytica, 2019) τον έκρινε θετικά, αλλά παρατήρησε τα εξής προβλήματα: Ότι δεν εφαρμόζεται παρά μόνο στις μεγάλες πολυεθνικές επιχειρήσεις, ότι στα μικρότερα κράτη - μέλη εφαρμόζεται πιο αργά από ό,τι στα μεγάλα, και έκρινε ότι η επιτυχία του GDPR θα εξαρτηθεί από το αν υπάρχουν αξιωματούχοι προστασίας δεδομένων και δικαστές που να αξιολογούν σοβαρά τις καταστάσεις στις οποίες το απόρρητο και η ελευθερία του τύπου φέρονται να συγκρούονται. Η έρευνα Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource (Joanna Kessler, 2019-2020:93-99) υποστηρίζει ότι οι Ηνωμένες Πολιτείες πρέπει να υιοθετήσουν ένα ομοσπονδιακό πρότυπο που να προσφέρει στους καταναλωτές παρόμοια ισχυρή προστασία με αυτήν του GDPR.

Σε μία έρευνα του 2015 ο S. Ciriani (Stephane Ciriani, 2015:41-58) μελέτησε τη μεγάλη πολυεθνική γαλλική εταιρεία τηλεφωνίας Orange και βρήκε ότι η εφαρμογή του Ευρωπαϊκού Δικαίου και σε χώρες εκτός Ευρωπαϊκής Ένωσης, όπως αποτελεσματικά κάνει ο GDPR, θα προωθούσαν ίσους όρους ανταγωνισμού στην Ευρωπαϊκή αγορά. Αλλά, με εξαίρεση την αξιολόγηση του GDPR που διενεργήθηκε από την ίδια την Ευρωπαϊκή Επιτροπή, άλλες

έρευνες κατέληξαν στο συμπέρασμα ότι το οικονομικό κόστος της εφαρμογής του αντισταθμίζει τα οφέλη από την αύξηση της αποδοτικότητας και εξέφρασαν την ανησυχία ότι η αύξηση του διοικητικού φόρτου ενδέχεται να μην συμβάλλει στη βελτίωση της ανταγωνιστικότητας των ευρωπαϊκών παροχών ψηφιακών υπηρεσιών. Για αυτό προτείνουν μια πιο ευέλικτη αντιμετώπιση από τους αξιωματούχους του GDPR.

Μια άλλη έρευνα (Sarah Shyy, 2020:137-164) υποστηρίζει ότι ο GDPR αποτυγχάνει να εξασφαλίσει το απόρρητο των καταναλωτών, επειδή στις σημερινές πρακτικές συλλογής δεδομένων οι καταναλωτές αναγκάζονται να αποδεχθούν την πολιτική απορρήτου της οποιασδήποτε διαδικτυακής εταιρείας και τις πρακτικές συλλογής δεδομένων τους. Εν τω μεταξύ, ο GDPR έχει θέσει σε μειονεκτική θέση τις μικρομεσαίες επιχειρήσεις επιβάλλοντας μέτρα απαγορευτικού κόστους, εμποδίζοντας την ανάπτυξη των μικρομεσαίων επιχειρήσεων, ωθώντας τις εν τέλει να εξέλθουν από την αγορά. Αντί να αντιγράψουν το μοντέλο του GDPR, υποστηρίζει, οι νομοθέτες των Η.Π.Α. θα πρέπει να διδαχθούν από τις αδυναμίες του GDPR και να υιοθετήσουν κανονισμούς που να είναι αποτελεσματικοί στην προστασία της ιδιωτικής ζωής των καταναλωτών, αλλά και να επιβαρύνουν λιγότερο τις επιχειρήσεις.

5.3 ΤΑ ΟΦΕΛΗ ΤΟΥ GDPR ΣΤΙΣ ΕΠΙΧΕΙΡΗΜΑΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Εντοπίζονται δύο εργασίες που δημοσιεύθηκαν το 2019 και εξετάζουν τον GDPR από επιχειρηματική σκοπιά (Nazar Poritskiy, Flávio Oliveira and Fernando Almeida,2019:510-524; Daria Dubrova, 2018). Οι εργασίες αυτές κατέληξαν στο συμπέρασμα ότι τα δύο πιο σημαντικά οφέλη ήταν η εμπιστοσύνη των καταναλωτών και το ότι διευκρινίστηκαν νομικά πρότερες γκρίζες ζώνες. Επιπλέον, θεώρησαν δευτερεύοντα οφέλη το ότι βοήθησε στη λήψη αποφάσεων, στην καλύτερη αξιολόγηση των κυβερνοκινδύνων,

στην αύξηση της ασφάλειας προϊόντων και υπηρεσιών και στη βελτίωση των διαδικασιών διαχείρισης δεδομένων.

Μια ακόμα εργασία (Gonçalo Almeida Teixeira, Miguel Mira da Silva and Ruben Pereira, 2019:402-418) διεξήγαγε μία βιβλιογραφική ανασκόπηση για τον εντοπισμό των κρίσιμων παραγόντων που συμβάλλουν σε μια επιτυχή εφαρμογή του GDPR. Ένα από τα ερωτήματα ήταν: ποια είναι τα οφέλη από τη συμμόρφωση με τον GDPR. Η ανασκόπησή τους εντόπισε τέσσερις πιθανούς τομείς όπου το GDPR τις ωφέλησε: 1) στη σωστή διαχείριση δεδομένων, 2) στη χρήση αναλυτικών δεδομένων, 3) στη μείωση κόστους και 4) στην αύξηση της καλής φήμης τους. Όσον αφορά τη διαχείριση δεδομένων Lopes και Oliveira (Isabel Maria Lopes and Pedro Oliveira, 2018) βλέπουν τον GDPR ως μία ευκαιρία για τις εταιρείες να βελτιώσουν τις μεθόδους καταγραφής και ελέγχων των διαδικασιών τους. Επίσης θεωρούν ότι είναι μία ευκαιρία για την επίτευξη συνοχής δεδομένων σε μία πολυεθνική οργάνωση. Άλλοι υποστηρίζουν ότι η βελτίωση στη διαχείριση δεδομένων θα εξαλείψει το πλεόνασμα των αποθηκευμένων δεδομένων και έτσι θα επιτευχθεί η μείωση του κόστους λειτουργίας των εταιρειών, λόγω του ότι δεν θα χρειάζεται να αποθηκευτούν αυτά τα δεδομένα σε server. Σύμφωνα με μια εκτίμηση της Ευρωπαϊκής Επιτροπής μπορούν να εξοικονομηθούν έως και 2,3 δισεκατομμύρια ευρώ στην Ευρώπη ετησίως (Ralph O'Brien, 2016:81-84).

Ο Beckett (Phil Beckett, 2017:9-13) υποστηρίζει ότι η συμμόρφωση με τον GDPR και οι δεξιότητες ασφαλούς επεξεργασίας δεδομένων μπορεί να ενισχύσουν την αξιοπιστία μιας εταιρείας και να δημιουργήσουν νέες επιχειρήσεις και νέους πελάτες προσφέροντας έτσι, ένα ανταγωνιστικό πλεονέκτημα σε αυτές τις εταιρείες (Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, 2018:134-156). Οι Garber and Miglicco πιστεύουν,

επίσης, ότι η συμμόρφωση με τον GDPR μπορεί να ενισχύσει την απόδοση ενός οργανισμού βελτιώνοντας τη λειτουργικότητά του (Joe Garber, 2018:14-15 & Gary Miglicco, 2018:9-12).

Με βάση τις προαναφερθείσες εργασίες οι ερευνητές έκριναν ότι, ενώ δήλωναν όλες οι εταιρείες που συμμετείχαν ενδιαφέρον για την προστασία προσωπικών δεδομένων, το κίνητρό τους ήταν ξεκάθαρα ο φόβος του προστίμου (4% του ετήσιου παγκόσμιου τζίρου τους ή 20 εκατομμύρια, όποιο είναι πιο υψηλό). Όπως παρατήρησε ένα στέλεχος «βάζει το σύνολο της εταιρείας σε διαφορετική νοοτροπία» (Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez, 2018:193-203).

Η υπαρξιακή απειλή γίνεται αισθητή τόσο για τις μεγάλες όσο και για τις μικρές εταιρείες. Ανώτερο στέλεχος μίας από τις μεγαλύτερες εταιρείες είπε : «κάνουμε προσομοιωμένες ασκήσεις στην αντιμετώπιση κρίσεων και πάντα καταλήγουν σε διαδικτυακή κυβερνοεπίθεση και διαρροή δεδομένων, όπου αυτά είναι τα δεδομένα με τα οποία διευθύνουμε την επιχείρησή μας. Για αυτό ένα τέτοιο σενάριο είναι ο μεγαλύτερός μου φόβος και με κρατάει ξύπνιο κάθε νύχτα». Ο οικονομικός διευθυντής μιας μικρομεσαίας επιχείρησης εξέφρασε πιο έντονα τον φόβο του προστίμου: ούτως ή άλλως η εταιρεία λειτουργεί με ψίχουλα, οπότε ακόμη και το παραμικρό λάθος θα ωθήσει στη χρεοκοπία.

Ο GDPR έχει κάνει τα ανώτερα στελέχη των εταιρειών να προσέχουν πολύ περισσότερο τα προσωπικά δεδομένα, τόσο σε εταιρικό όσο και σε προσωπικό επίπεδο. Ένα από αυτά τα στελέχη δηλώνει ότι: «είμαστε πολύ ενημερωμένοι για την αύξηση του GDPR, μας χτύπησε σαν ένα παλιρροιακό κύμα ρυθμίσεων, επειδή γνωρίζαμε ότι οι κυρώσεις εναντίον των εταιρειών που δεν το τηρούσαν θα ήταν αρκετά σκληρές. Και καταλάβαμε επίσης ότι

ήταν σημαντικό. Όλοι έχουμε προσωπική ζωή και ξέρουμε πώς είναι όταν λαμβάνουμε ενοχλητικές ειδοποιήσεις και καταγράφονται όλα τα προσωπικά δεδομένα μας από τις εταιρείες των υπηρεσιών που χρησιμοποιούμε. Με άλλα λόγια μεταχειριζόμαστε τα δεδομένα των πελατών μας όπως θα θέλαμε να μεταχειρίζονται τα δικά μας.

Ένας διαφημιστής όρισε την επίδραση που έχει ο GDPR ως εξής: «όσο επώδυνο και αν είναι, ουσιαστικά αυτό που μας επιτρέπει να κάνουμε είναι να κατανοήσουμε το επιθυμητό επίπεδο αλληλεπίδρασης των πελατών μας με την εταιρεία. Πριν, είχες μία απλή μάζα πελατών και συνήθιζες να επικοινωνείς μαζί τους με οποιοδήποτε μέσο και όποτε εσύ ήθελες. Κάποιοι από αυτούς ήταν πιο δεκτικοί και κάποιοι όχι τόσο» (Gerard Buckley, Tristan Caulfield; Ingolf Becker, 2021).

Με άλλα λόγια, ως επιχειρηματική πρακτική δεν υπάρχουν άλλα ανεπιθύμητα μηνύματα. Ο GDPR έχει αλλάξει την εταιρική νοοτροπία που πρότερα είχαν οι εταιρείες, η οποία ήταν: κρατάμε τα δεδομένα μήπως και μας είναι χρήσιμα στο μέλλον. Έχει αυξήσει την ευαισθητοποίηση εντός των επιχειρήσεων όσον αφορά τις κυβερνοεπιθέσεις, με αποτέλεσμα πολλές από αυτές να ασφαλίζουν την εταιρεία τους για αυτό το ενδεχόμενο. Ένας αναλυτής ανέφερε: «η ασφάλεια έχει αυξηθεί δραματικά όσον αφορά την κρυπτογράφηση. Εν ολίγοις ο GDPR έχει κάνει τις εταιρείες να γίνουν πιο υπεύθυνες. Όπως το έθεσε ένας διευθύνων σύμβουλος: «υποθέτω ότι είμαστε λίγο πιο προσεκτικοί για ποιο σκοπό χρησιμοποιούμε τα δεδομένα» (Gerard Buckley, Tristan Caulfield & Ingolf Becker, 2021).

Ο GDPR ενδέχεται να απαιτεί από τις εταιρείες να αλλάξουν τους υπαλλήλους της διαδικασίας ή την τεχνολογία τους. Εξαρτάται από το πόσο κοντά ήταν το μοντέλο λειτουργίας τους, αν ήταν ήδη ευθυγραμμισμένο με

τον νέο αυτό κανονισμό. Ας υποτεθεί ότι μια εταιρεία αναγκάζεται να αγοράσει ένα σύστημα δεδομένων για να ικανοποιήσει τον GDPR. Το νέο αυτό σύστημα βοηθάει και αυξάνει την αποδοτικότητα της εταιρείας, μειώνοντας έτσι και το κόστος λειτουργίας της. Σε αυτήν την περίπτωση είναι δύσκολο να υποστηριχθεί ότι η αύξηση αυτή στην αποτελεσματικότητα ήταν ένα άμεσο όφελος του GDPR. Διότι η εταιρεία θα μπορούσε να χρησιμοποιήσει τα ίδια χρήματα για κάτι που παράγει μεγαλύτερη αξία, όπως η ανάπτυξη νέων προϊόντων ή η επέκτασή της σε νέες αγορές.

Ωστόσο, αν μια εταιρεία αντιμετωπίζει μακροχρόνια ζητήματα που γνωρίζει ότι πρέπει να επιλυθούν, διαφορετικά θα υποβαθμιστεί ή θα καταστραφεί και το GDPR αποτελέσει το κίνητρο για να πραγματοποιηθεί τελικά αυτή η επένδυση, τότε πολύ εύκολα μπορεί να υποστηριχθεί ότι αυτό είναι ένα άμεσο όφελος για τις επιχειρήσεις (Gerard Buckley, Tristan Caulfield & Ingolf Becker, 2021).

Μία από τις μικρομεσαίες επιχειρήσεις είπε ότι το πιο σημαντικό όφελος του GDPR ήταν να βάλει τα πράγματα σε τάξη. Είχαμε αρκετά έγγραφα για να γεμίσουμε ένα γήπεδο, αλλά αναγκαστήκαμε να μετακινήσουμε τα πάντα στο cloud, μειώσαμε τη χρήση του χαρτιού, τελικά μειώνοντας τα έγγραφά μας κατά 2/3. Στην πραγματικότητα ο GDPR σημαίνει ψηφιοποίηση, αυτοματοποίηση όλων των συστημάτων και αναδιοργάνωση του οργανισμού.

Μία από τις μεγαλύτερες εταιρείες είχε ήδη καταλήξει στο συμπέρασμα ότι το μάρκετινγκ βασίζεται στα δεδομένα και ότι είναι ο δρόμος του μέλλοντος. Έτσι, χρησιμοποιεί τον GDPR ως ευκαιρία για να συγκεντρώσει όλες τις βάσεις δεδομένων των πελατών της κάθε χώρας σε μία παγκόσμια βάση και να τυποποιήσει τις διεργασίες εισαγωγής και εξόδου δεδομένων.

Έκανε πιο αυστηρούς τους ελέγχους πρόσβασης και αναβάθμισε την ασφάλεια των δεδομένων της. Επιπλέον απαίτησαν από όλους τους πελάτες τους να τους δώσουν ξανά τη συγκατάθεσή τους, ως μέρος μιας προσπάθειας να είναι έτοιμοι για τον GDPR. Άλλαξαν τις αρχές λειτουργίας της εταιρείας ώστε να εναρμονίζονται με τις αρχές του GDPR, έτσι ελαχιστοποίησαν τα συλλεγόμενα δεδομένα, μείωσαν τον χρόνο που τα κρατούσαν και έπειτα επέβαλαν αυτές τις αλλαγές και σε όλα τα υποκαταστήματα της εταιρείας, εκτός της Ευρωπαϊκής Ένωσης.

Για παράδειγμα, η εταιρεία έχει πλέον ένα αυτοματοποιημένο σύστημα που επισημαίνει και διαγράφει δεδομένα πελατών αν έχουν να συνδιαλλαγούν με την εταιρεία για πάνω από έναν χρόνο. Αυτός ο μηχανισμός έχει το πρόσθετο πλεονέκτημα ότι χρησιμοποιείται και ως ένας τρόπος επικοινωνίας μεταξύ της διοίκησης και του μάρκετινγκ. Δηλαδή μπορεί να πει η διοίκηση : «γιατί αμελήσατε να επικοινωνήσετε με αυτούς τους υποψήφιους πελάτες; Μήπως μια μαζική καμπάνια δεν στόχευσε το σωστό κοινό; Ο GDPR ώθησε στην καινοτομία; Πιθανώς (Gerard Buckley, Tristan Caulfield; Ingolf Becker, 2021).

Έξι εταιρείες που συμμετείχαν στην έρευνα είπαν ότι «ο GDPR τις οδηγεί να καινοτομούν» και να κάνουν τις εξής δράσεις: η τεχνολογική μικρομεσαία επιχείρηση είπε πως ο προμηθευτής τους έχει προσθέσει μία εγκατάσταση αυτοεξυπηρέτησης, ώστε οι πελάτες να μπορούν να επιβλέπουν και να επεξεργάζονται τα προσωπικά τους στοιχεία, δηλαδή ένα SAR do-it-yourself. Η δεύτερη εταιρεία, που διέθετε τεχνικούς υπολογιστών, παραδέχθηκε ότι είχαν αυξηθεί οι υπάρχοντες πελάτες της και δημιουργήθηκαν νέες επιχειρήσεις, οι οποίες πασχίζουν να αναπτύξουν νέες υπηρεσίες για να ανταποκριθούν στις απαιτήσεις των πελατών τους σχετικά με τον GDPR.

Παρομοίως, μια δικηγορική εταιρεία έπρεπε να προσθέσει επιπλέον προσωπικό για να χειριστεί υποθέσεις που αφορούσαν τον GDPR. Άνοιξε ένα νέο υποκατάστημα στις Η.Π.Α. για να συμβουλεύει τοπικές εταιρείες σχετικά με αυτόν και επέκτεινε μία υπηρεσία νομικής πλατφόρμας, με τεχνολογία συμβατή με τον GDPR, για τους πελάτες της που έπρεπε να πάρουν μία γενική πληροφόρηση σε διεθνή νομικά θέματα. Επίσης οι αναφορές από τις τράπεζες δείχνουν ότι ο αριθμός των εταιρειών στον τομέα των υπηρεσιών GDPR είχε επεκταθεί, γι' αυτό και τους παραχώρησε μια μεγάλη γκάμα νέων υπηρεσιών. Από τα προηγούμενα συμπεραίνουμε ότι ο GDPR έχει ωφελήσει σε μεγάλο βαθμό εταιρείες, που παρέχουν τεχνολογικές ή νομικές συμβουλές και υπηρεσίες συναφείς με τον GDPR.

Αλλά και για την πλειονότητα των εταιρειών, όπου ο GDPR δεν είναι η βασική επιχειρηματική δραστηριότητά τους, εξακολουθεί να έχει οφέλη. Η απειλή των προστίμων έχει αλλάξει τη νοοτροπία των εταιρειών αυτών. Σε έναν κόσμο, όπου τα προσωπικά δεδομένα γίνονται ολοένα και πιο σημαντικά, ο GDPR έχει αναγκάσει τις εταιρείες να σεβαστούν τις επιθυμίες των πελατών τους, δηλαδή να εξυπηρετούνται με τον τρόπο που θέλουν οι ίδιοι και τα δεδομένα τους να χρησιμοποιούνται μόνο με τον τρόπο που οι ίδιοι θα το επέτρεπαν. Έχει οδηγήσει τις εταιρείες σε μεγαλύτερη διαφάνεια, κάτι το οποίο είναι θετικό και για αυτές και για όλη την κοινωνία. Έχει αλλάξει την υποδομή των εταιρειών όσον αφορά τα δεδομένα, διότι τις έχει φέρει σε μια πραγματικότητα όπου το κόστος συμμόρφωσης με τις αρχές του GDPR είναι πολύ μικρότερο από το κόστος του προστίμου. Έτσι, τις έχει αναγκάσει να εκσυγχρονίσουν και να αναβαθμίσουν τη διαχείριση των δεδομένων τους, την ποιότητα και την ασφάλεια των πληροφοριών τους. Ο GDPR έχει δώσει στις εταιρείες έναν λόγο να επενδύσουν σε έργα όπως ο εξορθολογισμός των βάσεων δεδομένων παλαιού τύπου, που ενώ γνώριζαν ότι ήταν σημαντικά, ωστόσο

συνέχιζαν να αναβάλλουν ή να αγνοούν. Έχει αναβαθμίσει εταιρείες που ήταν τεχνολογικά ανεπαρκείς δίνοντάς τους αρκετά οφέλη στην αποδοτικότητά τους.

Επίσης ωφέλησε έμμεσα εταιρείες των οποίων η τεχνολογία ήταν μεν επαρκής, αλλά εξακολουθούσε να απαιτεί βελτιώσεις ως προς την τήρηση των κανονισμών του. Ο GDPR έχει προσφέρει μερικά πλεονεκτήματα τυποποίησης και έχει χρησιμοποιηθεί από ορισμένες εταιρείες ως μέσο, για να αποδείξουν τη δέσμευσή τους στην προστασία των προσωπικών δεδομένων, με απώτερο στόχο να τονίσουν το brand name (την επωνυμία) και τη φήμη τους.

Πρέπει, όμως, να προσθέσουμε ότι κάποιες έρευνες δεν επιβεβαιώνουν τους ισχυρισμούς ότι ο GDPR βελτίωσε την εμπιστοσύνη των καταναλωτών, πράγμα το οποίο θα προσέφερε ανταγωνιστικό πλεονέκτημα σε κάποιες εταιρείες ή θα διευκρίνιζε τα πάντα νομικά, ούτε ότι μειώθηκε το κόστος, όπως πολλοί υπέθεταν. Πάντως σίγουρα είχε τεράστιο αντίκτυπο στην ψυχολογία των εταιρειών (Gerard Buckley, Tristan Caulfield; Ingolf Becker, 2021).

5.4 ΣΥΜΠΕΡΑΣΜΑΤΑ

Εν κατακλείδι, ο GDPR είναι ένας κανονισμός που έχει σχεδιαστεί για να προστατέψει το απόρρητο των δεδομένων των πολιτών της Ε.Ε. Τα οφέλη για τον καταναλωτή και τη ρυθμιστική αρχή και τα μειονεκτήματα για τις επιχειρήσεις είναι σχετικά προβλέψιμα. Το σημαντικό είναι αν υπάρχουν οφέλη του GDPR για τις επιχειρήσεις και πώς μπορεί να επηρεάσουν τους διάφορους οργανισμούς και εταιρείες. Τέλος, συμπεραίνεται ότι η απειλή μεγάλων προστίμων έχει ενεργοποιήσει τους ιθύνοντες των επιχειρήσεων και τις έχει καταστήσει πιο ευαισθητοποιημένες ως προς το απόρρητο και τα προσωπικά δεδομένα. Ο GDPR έχει δώσει στις εταιρείες έναν λόγο για

να δικαιολογήσουν την επένδυση στον εκσυγχρονισμό των διαδικασιών διαχείρισης δεδομένων και ασφάλειας. Οι εταιρείες διαθέτουν πιο καθαρές, πιο καλά οργανωμένες και πιο ενημερωμένες βάσεις δεδομένων των πελατών τους. Ελλείψει του GDPR, οι εταιρείες παραδέχονται ότι θα ζητούσαν περισσότερες πληροφορίες από όσες χρειάζονταν, θα τις αποθήκευαν για πιο μεγάλο διάστημα και με λιγότερη ασφάλεια.

Επίσης ο GDPR έχει γίνει αφορμή για να θεσπιστούν από τις εταιρείες εσωτερικές ρυθμιστικές αρχές, οι οποίες επιβάλλουν την εφαρμογή των μέτρων και τον σεβασμό στην ιδιωτικότητα και θα συνεχίσουν να έχουν μεγάλη επιρροή στη λήψη εταιρικών αποφάσεων, αν φυσικά οι επίσημες ρυθμιστικές αρχές της Ε.Ε. διατηρήσουν μια σταθερή στάση και υποχρεώσουν πρόστιμα στους παραβάτες. Αλλά, φυσικά, διαπιστώνουμε ότι υπάρχουν και πολλά προβλήματα με την εφαρμογή του GDPR, που θα αντιμετωπίζονταν με καλύτερη επικοινωνία, καθοδήγηση και απλούστευση από την Ε.Ε. και το αρμόδιο ρυθμιστικό στέλεχός της. Συνοπτικά, ο GDPR μπορεί να είναι πονοκέφαλος για τις επιχειρήσεις, αλλά τις έχει κάνει πιο προσεκτικές με τα δεδομένα. Κρίνοντας από το αποτέλεσμα ο GDPR ήταν ένας επιτυχημένος κοινωνικό- τεχνικός κανονισμός (Gerard Buckley, Tristan Caulfield;Ingolf Becker, 2021).

ΚΕΦΑΛΑΙΟ 6: GDPR, ΨΗΦΙΑΚΗ ΗΘΙΚΗ ΚΑΙ ΜΑΖΙΚΗ ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σχετικά με την Ψηφιακή Διακυβέρνηση πολλά μπορούν να ειπωθούν, αλλά είναι σαφές ότι η διακυβέρνηση του ψηφιακού κόσμου, η ψηφιακή ηθική – υπολογιστική ηθική ή ηθική δεδομένων – (Floridi L, Taddeo M., 2016) και η νομοθέτηση του ψηφιακού κόσμου είναι διαφορετικές προσεγγίσεις και δεν πρέπει να συγχέονται μεταξύ τους, αλλά να διακρίνονται ξεκάθαρα.

Η ψηφιακή διακυβέρνηση είναι ο μηχανισμός θέσπισης και εφαρμογής των πολιτικών και των διαδικασιών με σκοπό τη σωστή ανάπτυξη, χρήση και διαχείριση των πληροφοριών. Είναι ένα θέμα που απαιτεί καλό συντονισμό και βρίσκεται εκτός των ορίων της συμβατικής ηθικής και νομοθεσίας. Για παράδειγμα, μέσω της ψηφιακής διακυβέρνησης, μια κρατική υπηρεσία ή μια εταιρεία μπορεί να καθορίζει και να ελέγχει τις διαδικασίες και τις μεθόδους, που χρησιμοποιούνται από τους διαχειριστές δεδομένων, προκειμένου να βελτιώσει την ποιότητα των δεδομένων, την αξιοπιστία, την ευκολία πρόσβασης, την ασφάλεια των υπηρεσιών της, ώστε, έτσι, να επινοήσει αποτελεσματικές διαδικασίες, να επιταχύνει τη λήψη αποφάσεων και τον προσδιορισμό των ευθυνών, όσον αφορά τις διαδικασίες που σχετίζονται με τα δεδομένα.

Ένα παράδειγμα στο οποίο βλέπουμε μια τυπική εφαρμογή της ψηφιακής διακυβέρνησης είναι στο Βρετανικό Υπουργικό Συμβούλιο του 2016 σχετικά με τη δημιουργία ενός « πλαισίου δεοντολογίας της επιστήμης δεδομένων» (Cabinet Office, 2016), το οποίο προοριζόταν

να παρέχει καθοδήγηση στους δημοσίους υπαλλήλους για τη διεκπεραίωση έργων, που χρησιμοποιούσαν μεθόδους της επιστήμης δεδομένων, δίνοντάς τους ,έτσι, αυτοπεποίθηση να καινοτομήσουν με τα δεδομένα. Παρά την ονομασία του συμβουλίου, πολλές συστάσεις δεν είχαν καμία σχέση με ηθική και αφορούσαν απλώς τη διακυβέρνηση. Η ψηφιακή διακυβέρνηση μπορεί να περιλαμβάνει κατευθυντήριες γραμμές και συστάσεις, που επικαλύπτονται με τους κανονισμούς χρήσης ψηφιακών δεδομένων, αλλά δεν είναι πανομοιότυπες με αυτόν.

Αυτός είναι απλώς ένας άλλος τρόπος να μιλήσουμε για τη σχετική νομοθεσία, ένα σύστημα νόμων, που εκπονούνται και επιβάλλονται μέσω κοινωνικών ή κυβερνητικών θεσμών για τη ρύθμιση της συμπεριφοράς των οργανισμών - εταιρειών στον τομέα της πληροφορικής. Όχι ότι κάθε πτυχή των ψηφιακών κανονισμών είναι θέμα ψηφιακής διακυβέρνησης και ούτε κάθε πτυχή της ψηφιακής διακυβέρνησης είναι ψηφιακός κανονισμός. Σε αυτή την περίπτωση, ένα καλό παράδειγμα παρέχεται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation, 2016). Η συμμόρφωση είναι η κρίσιμη σχέση μέσω της οποίας ο ψηφιακός κανονισμός διαμορφώνει την ψηφιακή διακυβέρνηση.

Η ψηφιακή ηθική είναι ο κλάδος της ηθικής που μελετά και αξιολογεί α. τα ηθικά προβλήματα που σχετίζονται με τη χρήση των δεδομένων και των πληροφοριών (συμπεριλαμβανομένων της δημιουργίας, καταγραφής, επιμέλειας, επεξεργασίας, διάδοσης, κοινής χρήσης), β. τους αλγόριθμους (συμπεριλαμβανομένων της τεχνητής νοημοσύνης,

τεχνητών παραγόντων, μηχανής μάθησης και ρομπότ) και γ. τις αντίστοιχες πρακτικές και υποδομές (συμπεριλαμβανομένων των υπεύθυνων για καινοτομία, προγραμματισμό, hacking, επαγγελματικούς κώδικες και πρότυπα), προκειμένου να διατυπώσουν και να υποστηρίξουν ηθικά ορθές λύσεις (π.χ. ορθή συμπεριφορά και ηθικές αξίες), (Floridi L, Taddeo M. 2016). Οι αρχές της ψηφιακής ηθικής είναι η ψηφιακή ρύθμιση και η ψηφιακή διακυβέρνηση και μέσα από τη σχέση της ηθικής και της νομοθεσίας στοχεύει να πετύχει το προτιμητέο για την κοινωνία.

Η ψηφιακή διακυβέρνηση είναι μόνο μία από τις τρεις κανονιστικές δυνάμεις, που μπορούν να διαμορφώσουν και να καθοδηγήσουν την ανάπτυξη του ψηφιακού κόσμου. Μόλις γίνει κατανοητή η αλληλεπίδρασή της με την ψηφιακή ηθική και την ψηφιακή ρύθμιση, (τις άλλες δύο κανονιστικές δυνάμεις), οι συνέπειες γίνονται προφανείς και καταλήγουμε στο συμπέρασμα ότι η συμμόρφωση με τη νομοθεσία είναι απαραίτητη, αλλά ανεπαρκής συνθήκη στο δρόμο για έμπρακτα αποτελέσματα στην κοινωνία.

Οι υπεύθυνοι χάραξης πολιτικής, τόσο σε πολιτικό όσο και σε επιχειρηματικό πλαίσιο, μπορεί να αναρωτιούνται γιατί πρέπει να εμπλακούν σε συζητήσεις ηθικής, όταν η νομική συμμόρφωση είναι η λύση (αυτό είναι ένα επαναλαμβανόμενο θέμα στη συζήτηση του GDPR, για παράδειγμα). Η απάντηση πρέπει να είναι σαφής: η συμμόρφωση είναι απαραίτητη, αλλά ανεπαρκής για να οδηγήσει την κοινωνία στη σωστή κατεύθυνση, διότι η ψηφιακή ρύθμιση ορίζει ποιες είναι οι νόμιμες και οι παράνομες κινήσεις στο

επιχειρηματικό σκάκι, δεν αναφέρει, όμως, ποιες είναι οι καλές και οι κάλλιστες κινήσεις, που θα μπορούσαν να σε οδηγήσουν στο να κερδίσεις το παιχνίδι, δηλαδή να έχεις μια καλύτερη κοινωνία. Αυτό είναι το καθήκον τόσο της ψηφιακής ηθικής, από την πλευρά των ηθικών αξιών και προτιμήσεων, όσο και της καλής ψηφιακής διακυβέρνησης, συνοδευόμενης από καλή διαχείριση. Και γι' αυτό, για παράδειγμα, η Ευρωπαϊκή Εποπτεία Προστασίας Δεδομένων (ΕΕΠΔ), η ανεξάρτητη αρχή προστασίας δεδομένων της Ε.Ε., ίδρυσε τη Συμβουλευτική Ομάδα Δεοντολογίας το 2015, προκειμένου να εξετάσει τις νέες ηθικές προκλήσεις που εγείρονται από τις ψηφιακές εξελίξεις και την ισχύουσα νομοθεσία, ιδίως σε σχέση με τον GDPR.

Η ψηφιακή ηθική μπορεί να χωριστεί σε δύο τομείς, τη σκληρή και την ήπια ηθική. Στον πραγματικό κόσμο, η ήπια και η σκληρή ηθική συχνά συμπλέκονται άρρηκτα. Η σκληρή ηθική είναι αυτό που συνήθως έχει κατά νου κάποιος, όταν συζητάει για αξίες, δικαιώματα, καθήκοντα και ευθύνες ή γενικότερα, τι είναι ηθικά σωστό ή λάθος, κατά τη διαμόρφωση νέων κανονισμών ή προκλήσεων. Για παράδειγμα, στη σκληρή ηθική συμπεριλαμβάνονται οι προσπάθειες για τη δημιουργία ή αλλαγή μιας νομοθεσίας, όπως αυτές, για παράδειγμα, που τελείωσαν το Απαρτχάιντ στην Αφρική ή αυτές που έφεραν ισότητα για τις γυναίκες στον εργασιακό χώρο.

Εν ολίγοις, στον βαθμό που η ηθική συμβάλλει στη δημιουργία, τη διαμόρφωση ή την αλλαγή του νόμου, μπορεί να ονομαστεί σκληρή ηθική. Η ήπια ηθική αφορά τα ίδια θέματα με τη σκληρή ηθική, αλλά

το κάνει εξετάζοντας τι πρέπει και τι δεν πρέπει να γίνει πέρα και από την υπάρχουσα νομοθεσία, χωρίς να προσπαθεί να πάει κόντρα σε αυτήν, να την αλλάξει ή να την παρακάμψει, π.χ. η αυτορρύθμιση. Με άλλα λόγια, η ήπια ηθική είναι ηθική μετά τη συμμόρφωση με τον νόμο.

Ένα παράδειγμα που δείχνει τον ρόλο της ηθικής όσον αφορά τον GDPR είναι το ακόλουθο: Ο GDPR αποτελείται από 99 άρθρα, πράγμα το οποίο τον καθιστά ιδιαίτερα πολύπλοκο και λόγω αυτής της πολυπλοκότητας του κανονισμού, αλλά και του ευρέος φάσματος των περιπτώσεων που καλύπτει (ιδιαίτερα εδώ που νομοθετεί την ταχέως εξελισσόμενη τεχνολογία), ο κανονισμός (σκληρή ηθική) αδυνατεί να καλύψει τα πάντα και δημιουργεί γκρίζες ζώνες και αβεβαιότητα. Τότε, λοιπόν, αναλαμβάνει ρόλο η ήπια ηθική, για την εποικοδομητική ερμηνεία αυτών των κενών στον κανονισμό. Επιπλέον, οποιαδήποτε ηθική προσέγγιση στην Ε.Ε. έχει ως προαπαιτούμενο την εφαρμογή της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου, την Ευρωπαϊκή Σύμβαση για τα Ανθρώπινα Δικαιώματα και τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης**.**

Όπως τονίστηκε παραπάνω, τόσο η σκληρή όσο και η ήπια ηθική προϋποθέτουν σκοπιμότητα. Η ηθική δεν πρέπει να είναι καθαρά θεωρητική και να ζητά κάτι το αδύνατο. Κατά συνέπεια στην Ε.Ε., όπου έχει εφαρμοστεί ο GDPR, η σκληρή ηθική έχει κάνει το έργο της και τώρα είναι η στιγμή της ήπιας ηθικής να δράσει με μια νέα προσέγγιση (σκοπιμότητα), ώστε να επιτευχθούν τα επιθυμητά

αποτελέσματα στην κοινωνία. Για αυτό θα πρέπει να συζητηθεί ο ηθικός αντίκτυπος της χρήσεως και καταχρήσεως δεδομένων από τους διάφορους οργανισμούς, αλλά, ίσως, και η υπερβολική ισχύς του κανονισμού, ώστε να είναι σε θέση να εφαρμόσουμε την ήπια ηθική αποτελεσματικά (Luciano Floridi, 2018).

6.1 GDPR ΚΑΙ ΚΛΕΙΣΤΑ ΚΥΚΛΩΜΑΤΑ ΒΙΝΤΕΟΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

Οι διατάξεις του Νόμου για την προστασία των προσωπικών δεδομένων δεν εφαρμόζονται στην περίπτωση εγκατάστασης Κλειστών Κυκλωμάτων Βιντεοπαρακολούθησης σε ιδιωτικούς χώρους, όπως οικίες ή πολυκατοικίες, επειδή η επεξεργασία τους πραγματοποιείται από φυσικό πρόσωπο και αφορά σε δραστηριότητες προσωπικές ή οικιακές. Ωστόσο, η εμβέλεια καταγραφής του ΚΚΒΠ δεν πρέπει να είναι εκτός της περιμέτρου του ιδιωτικού χώρου. Ο Γενικός Κανονισμός Προστασίας των Δεδομένων, όμως, μπορεί να συνάπτει συμβάσεις με τις Εταιρείες Διαχείρισης των κοινόχρηστων οικοδομών, ώστε να συντηρεί και να διαχειρίζεται από κοινού με αυτές το βιντεοσκοπημένο υλικό .

Ο Κανονισμός τονίζει ότι δεν επιτρέπεται σε καμία περίπτωση να ελέγχεται η προσωπική συμπεριφορά, οι προσωπικές επαφές και η αποδοτικότητα των ατόμων μέσω τέτοιων συστημάτων. Τα δεδομένα διατηρούνται για εύλογο χρονικό διάστημα, πάντα σε σχέση με το σκοπό που εξυπηρετούν, ενώ τα άτομα τα οποία καταγράφονται από ΚΚΒΠ μπορούν να ασκήσουν το δικαίωμα πρόσβασης.

Χαρακτηριστικά αναφέρεται ότι η σήμανση με τη χρήση προειδοποιητικών πινακίδων είναι υποχρεωτική. Οι προειδοποιητικές πινακίδες θα πρέπει να είναι σε εμφανή σημεία, επαρκείς σε αριθμό και ευδιάκριτες από τα άτομα που καταγράφονται. Στις εν λόγω πινακίδες πρέπει να αναγράφεται (α) ότι

γίνεται βιντεοσκόπηση, (β) ο σκοπός της βιντεοσκόπησης και (γ) τα στοιχεία του υπεύθυνου επεξεργασίας (Υπουργείο Δικαιοσύνης, 2018).

6.2 ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ - Η ΠΕΡΙΠΤΩΣΗ ΤΟΥ FACEBOOK

Η μεγαλύτερη διαρροή προσωπικών δεδομένων, που έχει καταγραφεί μέχρι σήμερα, είναι αυτή των δεδομένων περισσότερων από 50 εκατομμυρίων χρηστών του Facebook, τα οποία χρησιμοποιήθηκαν για τη δημιουργία ενός προγράμματος λογισμικού, προκειμένου να επηρεαστούν οι ψηφοφόροι στις αμερικανικές εκλογές του 2016 υπέρ του Ντόναλντ Τραμπ, κατά την προεκλογική περίοδο (Τι συνέβη με το Facebook και τη μεγαλύτερη διαρροή προσωπικών δεδομένων, 2018).
Η εταιρεία ανάλυσης δεδομένων Cambridge Analytica αγόρασε τα δεδομένα όλων αυτών των χρηστών από έναν Ρώσο ακαδημαϊκό από το πανεπιστήμιο του Cambridge.

Σύμφωνα με τον Guardian ο ακαδημαϊκός αυτός δημιούργησε το 2014 μία εφαρμογή για το Facebook, στην οποία καλούνταν πολλές χιλιάδες χρήστες να απαντήσουν σε ένα τεστ προσωπικότητας για ακαδημαϊκούς λόγους. Ανταποκρίθηκαν 270.000 χρήστες και μέσω του προφίλ τους στο Facebook αυτός κατάφερε να έχει πρόσβαση και στο προφίλ και τα προσωπικά δεδομένα όλων των φίλων τους, δηλαδή περισσότερων από 50 εκατομμυρίων χρηστών ενώ το ίδιο το Facebook αναφέρει ότι πρόκειται για 87 εκατομμύρια χρήστες. Για το Facebook, όμως, αυτό αποτέλεσε παραβίαση των όρων χρήσης, καθώς δεν επιτρεπόταν στην εφαρμογή να χρησιμοποιήσει τα στοιχεία για εμπορικούς σκοπούς.

Όταν κλήθηκε από τις παγκόσμιες αρχές να απολογηθεί για το σκάνδαλο, δήλωσε: «Συνολικά, εκτιμάται ότι οι προσωπικές πληροφορίες έως και 87 εκατομμυρίων χρηστών, οι περισσότεροι εκ των οποίων βρίσκονται στις

ΗΠΑ, αποκτήθηκαν αθέμιτα από την Cambridge Analytica». Η εταιρεία κατανοεί τη σοβαρότητα του ζητήματος και ο πρόεδρός της Ζούκερμπεργκ αναλαμβάνει την ευθύνη για την αθέμιτη πρόσβαση στα προσωπικά δεδομένα των χρηστών (Facebook: Υποκλαπέντα δεδομένα 87 εκατ. Χρηστών, 2018). Μετά το σκάνδαλο, ο πρόεδρος του Facebook ανέφερε τα νέα σχέδιά του για πιο αυστηρή πολιτική προστασία των προσωπικών δεδομένων των χρηστών και για μεγαλύτερη διαφάνεια. Τέλος, ο Ζούκερμπεργκ είπε το εξής: «Νομίζω ο GDPR γενικώς θα είναι πολύ θετικό βήμα για το ιντερνέτ» (Πώς θα επηρεάσει το GDPR το Facebook, τα social media και εσάς, 2018).

Το Facebook έχει αρχίσει να ενημερώνει τους Ευρωπαίους χρήστες του για τροποποιήσεις στους όρους χρήσης, ώστε να συμμορφωθεί προς την ευρωπαϊκή νομοθεσία περί προστασίας δεδομένων, τον GDPR . Όπως όλα τα κοινωνικά μέσα δικτύωσης, σπεύδει να επικαιροποιήσει τις πολιτικές απορρήτου και οφείλει να λάβει τη συγκατάθεση των χρηστών του για τα προσωπικά τους δεδομένα(Πώς θα επηρεάσει το GDPR το Facebook, τα social media και εσάς, 2018).

6.3 ΑΛΛΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τον Ιανουάριο του 2019, η Γαλλική εποπτική αρχή προστασίας δεδομένων επέβαλε πρόστιμο πενήντα εκατομμυρίων ευρώ στη Google, για παραβίαση του GDPR. Η αρχή της Γαλλίας διαπίστωσε ότι στους χρήστες Android δεν εξηγούσε η Google με σαφήνεια τι πληροφορίες συλλέγει και για ποιους σκοπούς και δεν λάμβανε τη συγκατάθεση των χρηστών για κάθε περίπτωση. Το πόρισμα εναντίον της Google είναι η έλλειψη διαφάνειας, ανεπαρκής πληροφόρηση και έλλειψη έγκυρης συναίνεσης όσον αφορά στην εξατομίκευση των διαφημίσεων. Η εταιρεία βρίσκεται υπό έρευνα και από τις ιρλανδικές Αρχές.

Άλλο μεγάλο πρόστιμο ύψους 400.000 ευρώ επιβλήθηκε από τις πορτογαλικές Αρχές σε νοσοκομείο του οποίου το προσωπικό χρησιμοποιούσε ψευδείς λογαριασμούς για να αποκτήσει πρόσβαση στα δεδομένα ασθενών. Από τις πολωνικές Αρχές επιβλήθηκε πρόστιμο ύψους 220.000 ευρώ σε εταιρεία που συνέλεγε προσωπικά δεδομένα μέσω του διαδικτύου για διαφημιστικούς λόγους (Ένας χρόνος εφαρμογής του GDPR. Τι έγινε, τι θα γίνει, τι πρέπει να γίνει, 2019).

Ακόμα ένα άλλο περιστατικό συνέβη με την εταιρεία κινητής τηλεφωνίας Cosmote το 2020, όπου η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) της επέβαλε πρόστιμο έξι εκατομμυρίων ευρώ, για διαρροή προσωπικών δεδομένων. Βέβαια, η συγκεκριμένη εταιρεία υποστήριξε ότι ήταν αποτέλεσμα κυβερνοεπίθεσης. Μετά από δυο χρόνια διερεύνησης της υπόθεσης της επιβλήθηκε και η κύρωση διακοπής επεξεργασίας και καταστροφής των δεδομένων, λόγω διαρροής δεδομένων κλήσεων χιλιάδων συνδρομητών της, κατά το χρονικό διάστημα από 1/9/2020 έως 5/9/2020. Επίσης, με την ίδια απόφαση η ΑΠΔΠΧ επέβαλε πρόστιμο των 3.250.000 ευρώ και στον Οργανισμό Τηλεπικοινωνιών Ελλάδος (ΟΤΕ) (dpa.gr,2022).

ΚΕΦΑΛΑΙΟ 7: ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ ΕΦΑΡΜΟΓΗΣ ΤΟΥ GDPR

7.1 ΣΥΜΜΕΤΟΧΗ ΠΟΛΙΤΩΝ ΣΤΟ ΨΗΦΙΑΚΟ ΚΡΑΤΟΣ ΠΡΟΝΟΙΑΣ, Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ ΟΛΛΑΝΔΙΑΣ

Ο «κοινωνικός τομέας» των Ολλανδικών δήμων περιλαμβάνει τις υπηρεσίες κοινωνικών παροχών, υπηρεσίες φροντίδας για νέους, υποστήριξη χρέους, φροντίδας για ευάλωτα άτομα και άτομα που αναγκάστηκαν να εγκαταλείψουν πρώιμα το σχολείο. Πολλοί δήμοι στην Ολλανδία, ειδικά οι μεγάλοι, προσπαθούν να βρουν πώς να κάνουν καλύτερη χρήση των δεδομένων και αυτές οι δοκιμές τους θα παρουσιαστούν παρακάτω. Όπως θα δούμε, αυτή η λεπτομερής περιγραφή οδηγεί σε εποικοδομητική κριτική σχετικά με την επεξεργασία δεδομένων, που έχει σκοπό να βοηθηθούν οι δήμοι στη λειτουργία τους χρησιμοποιώντας δεδομένα. Αλλά, παρόλες τις καλές προθέσεις, συχνά τέτοια χρήση δεδομένων στην κοινωνική πολιτική αποτυγχάνει και δημιουργεί προβλήματα, όπως δείχνει η έρευνα της Eurobank (2018), για αυτό πρέπει να υπάρχει δημόσια συζήτηση και ενδεχομένως, παρέμβαση.

Κατά τη διάρκεια των τελευταίων 5 ετών οι δήμοι της Ολλανδίας εξετάζουν το ερώτημα πώς τα «big data», όπως το αποκαλούν οι ίδιοι, μπορούν να συμβάλουν στην επιτυχή υλοποίηση των δημοτικών καθηκόντων ως προς την κοινωνική πολιτική. Το θέμα των «big data» διερευνήθηκε εκτενώς από την Τοπική Αυτοδιοίκηση της Ολλανδίας λόγω της αποκέντρωσης που εφαρμόζει η χώρα στην κοινωνική της πολιτική, αλλά και για να χρησιμοποιηθούν ως εργαλείο για την καλύτερη κατανόηση των οικονομικών και κοινωνικών αλλαγών της χώρας. Εκείνη την εποχή, η εθνική κυβέρνηση μεταβίβασε την ευθύνη για τη φροντίδα των νέων, την κοινωνική ασφάλιση και τη φροντίδα για χρόνια πάσχοντες και ηλικιωμένους στους δήμους. Η αλλαγή αυτή αποσκοπούσε στο να φέρει

την κρατική βοήθεια πιο κοντά στους πολίτες καθιστώντας την ,έτσι, πιο φθηνή, αποτελεσματική και γρήγορη. Μετά από 3 χρόνια, ωστόσο, οι εθνικές, περιφερειακές και δημοτικές κυβερνήσεις κατέληξαν στο συμπέρασμα ότι αυτή η μετάβαση δεν είχε ακόμη ολοκληρωθεί και δεν είχε φτάσει σε όλους.

Οι φιλοδοξίες του προϋπολογισμού, επίσης, δεν είχαν επιτευχθεί αφού το κόστος της κοινωνικής πολιτικής το έτος 2017 αυξήθηκε αντί να μειωθεί. Οι προσδοκίες για το 2018 και το 2019 δεν ήταν διαφορετικές (Bekker H, 2018; Steiner, 2018a,b,). Σε αυτό το πλαίσιο, δεν αποτελεί έκπληξη το γεγονός ότι οι τοπικές κυβερνήσεις αναζητούν διαρκώς μέσα για να κάνουν έλεγχο της εφαρμογής και του κόστους της κοινωνικής πολιτικής. Η βελτιωμένη χρήση των ήδη υπαρχόντων και νέων ειδών δεδομένων, σε συνδυασμό με την έξυπνη σύνδεση δεδομένων και τις αναλυτικές τεχνικές θεωρείται ευρέως ότι έχει μεγάλες προοπτικές. Ο διευθυντής της Ένωσης Ολλανδικών Δήμων (VNG) δήλωσε ότι τα δεδομένα «παρέχουν μια εικόνα της πραγματικότητας και δημιουργούν τη δυνατότητα προσαρμογής της πολιτικής με καλά μελετημένο τρόπο όταν τα πράγματα πάνε λάθος» (Kriens, 2016).

Με τη χρήση αυτών των δεδομένων παρέχεται η δυνατότητα να ληφθούν δραστικές αποφάσεις, οι οποίες βοηθούν πολύ περισσότερο από την κομματική πολιτική και λέει επίσης ότι «οι δήμοι θα πρέπει να αποδεχθούν τις πληροφορίες» (Kriens, 2016). Το Ίδρυμα Stimulansz, ένας ιδρυματικός σύμβουλος Ολλανδικών δήμων, δηλώνει ότι «η σύνδεση δεδομένων μπορεί να σας βοηθήσει ως Δήμο να εργαστείτε ακόμα καλύτερα, με ακρίβεια και αποτελεσματικότητα. Για παράδειγμα στον εντοπισμό πλαστογραφιών ή στην επίβλεψη της ρύθμισης χρεών» (Stimulansz n.d., 2019). Αρκετοί άλλοι μεγάλοι σύμβουλοι και τοπικές μικρές και μεσαίες επιχειρήσεις

προσφέρουν τις υπηρεσίες τους στους δήμους για να τους βοηθήσουν να οργανώσουν και να συνδέσουν τα δεδομένα τους και να πειραματιστούν με σχετικές εφαρμογές.

Οι δήμοι συλλέγουν και διαχειρίζονται αμέτρητα προσωπικά δεδομένα ξεκινώντας από πολλές βασικές διοικητικές πράξεις που αποτελούν μέρος της Ολλανδικής νομοθεσίας (για άτομα, εισόδημα και οχήματα), όπως η παροχή υπηρεσιών και η έκδοση αδειών. Άτομα που πληρούν τις προϋποθέσεις για μια υπηρεσία του τομέα κοινωνικής πολιτικής, υποχρεούνται να υποβάλουν μια ολόκληρη σειρά προσωπικών δεδομένων. Στον τομέα αυτό, σχετικά με την υποχρέωση παροχής πληροφοριών, ισχύει η πράξη συμμετοχής. Επιπλέον, ορισμένοι δήμοι αγοράζουν πρόσθετα, ανώνυμα δεδομένα από εμπορικά μέρη (Hartholt S.,2017). Ο πιο σημαντικός συνεργάτης σε εφαρμογές δεδομένων είναι το Ολλανδικό Γραφείο Στατιστικής (CBS), το οποίο διαθέτει πολλά δεδομένα από τον τομέα της κοινωνικής πολιτικής, που έχει στη διάθεσή του, και προσφέρει την τεχνογνωσία του στους δήμους μέσω των Αστικών και Αγροτικών Κέντρων Δεδομένων.

Στην Ολλανδία, το ταμπλό της Ολλανδικής Ένωσης Δήμων (VNG) επιτρέπει στους δήμους να συγκρίνουν τη θέση τους με δήμους στις υπόλοιπες Κάτω Χώρες σε ένα ευρύ φάσμα δεικτών, ένας από τους οποίους είναι η Δημοτική Κοινωνική Πολιτική Παρακολούθησης του Τομέα. Τα δεδομένα που εμπλέκονται προέρχονται από το αρχείο περί κοινωνικής υποστήριξης, το οποίο δίνουν οι ίδιοι δήμοι στο CBS κάθε έξι μήνες. Στη συνέχεια, συμπληρώνονται με δεδομένα σχετικά με (μεταξύ άλλων) το εισόδημα, τη σύνθεση του νοικοκυριού και το προφίλ γειτονιάς. Από τους συνολικά 380 δήμους, οι 312 έχουν υποβάλει τα στοιχεία τους.

Η πλατφόρμα αυτή επεκτείνεται τακτικά με νέους δείκτες, όπως η πρόσφατα προστεθείσα «Ανάλυση διαδρομής ζωής», η οποία υποδεικνύει πώς χρησιμοποιούνται διαχρονικά οι κοινωνικές παροχές. Τα δεδομένα είναι ψευδοανώνυμα και συγκεντρώνονται σύμφωνα με κανόνες. Οι χρήστες μπορούν να πραγματοποιήσουν τις δικές τους αναλύσεις και οπτικοποιήσεις σε αυτά τα συγκεντρωτικά δεδομένα. Με την πλατφόρμα αυτή, το VNG ελπίζει να βοηθήσει τους δήμους με τον εντοπισμό και την κατεύθυνση των εξελίξεων στον τομέα της κοινωνικής πολιτικής, την αναμόρφωση της πολιτικής, την παράδοση πληροφοριών σχετικά με τη διαφάνεια στο δημοτικό συμβούλιο και στους πολίτες και να δώσει ένα μέτρο σύγκρισης μεταξύ των δήμων (Liesbet van Zoonen, 2020).

Ο τομέας κοινωνικής πολιτικής γνωρίζει δύο πανεθνικά συστήματα σύζευξης δεδομένων για τη διερεύνηση υπόπτων απατών: το σύστημα (SyRI), το οποίο στοχεύει πολίτες που ενδέχεται να διαπράξουν απάτη για παροχές και το αντίστοιχο (healthcare information hab), το οποίο εστιάζει σε επικίνδυνους παρόχους υγειονομικής περίθαλψης. Και τα δύο συστήματα λειτουργούν με βάση τις αναφορές που δίνονται από ενδιαφερόμενους αξιωματούχους, πολίτες ή ιδρύματα που υποπτεύονται ότι πρόκειται για απάτη. Μέχρι στιγμής, η πρόβλεψη απάτης ή άλλης προβληματικής συμπεριφοράς εμφανίζεται μόνο με τη μορφή πειράματος. Ένα πολύ γνωστό παράδειγμα μεταξύ των Ολλανδικών δήμων προέρχεται από τον δήμο του Zaanstad, όπου έλαβε χώρα μια δίκη για την πρόληψη της ενδοοικογενειακής βίας με βάση στοιχεία από τις αναφορές της αστυνομίας, τη Βάση Δεδομένων Προσωπικών Αρχείων (BRP), την Κοινωνική Ασφάλιση, την παροχή συμβουλών για χρέη, περιοριστικές εντολές και χρήση Υπηρεσιών.

Η εταιρεία που συνέλεξε και επεξεργάστηκε τα δεδομένα κατέληξε στο συμπέρασμα ότι τα δεδομένα δεν ήταν επαρκώς λεπτομερή και δεν εμφανίστηκε κάποιο μοτίβο (Noord-Hollands Dagblad, 2015). Άλλα προβλήματα, για τα οποία ελπίζουν οι δήμοι να βοηθηθούν, είναι η πρόωρη εγκατάλειψη του σχολείου, η συσσώρευση χρέους ,οι κίνδυνοι απάτης και η εγκληματική δράση (Bouman K., 2016).

Στην Ολλανδία, ο δικηγορικός σύλλογος παρατηρεί ότι ορισμένοι δήμοι δυσκολεύουν σκόπιμα τους ανθρώπους να κάνουν αίτηση για κοινωνική ασφάλιση ζητώντας τους ένα ακραίο όγκο δεδομένων (Rubio AI, 2018). Το 2017, το καταναλωτικό τηλεοπτικό πρόγραμμα Radar παρουσίασε την περίπτωση μιας γυναίκας με κοινωνικές παροχές που κατηγορήθηκε για απάτη επειδή φρόντιζε τη μητέρα της με άνοια και δεν είχε συμπεριλάβει τις αποταμιεύσεις της μητέρας της στο δικό της δηλωθέν εισόδημα. Όπως αποδείχθηκε, το σύστημα έκανε συχνά τέτοια λάθη (Radar, 2017). Τέτοια παραδείγματα δείχνουν ότι η μέτρηση της ανεξάρτητης μεταβλητής του «κινδύνου απάτης» βασίζεται στις υπάρχουσες περιπτώσεις απάτης που δεν είναι απαραίτητα έγκυρες.

Μετά από όλα αυτά, είναι άγνωστο εάν η μέτρηση βασίζεται σε μια σωστή ή εσφαλμένη ερμηνεία της διοικητικής παρατυπίας. Αυτό καθιστά αναξιόπιστες όλες τις προγνωστικές αναλύσεις που χρησιμοποιούν αυτήν τη μεταβλητή. Γενικότερα, υπάρχει ελάχιστη εικόνα για τον τρόπο με τον οποίο οι δήμοι οργανώνουν, επεξεργάζονται και καταχωρούν τα δεδομένα στον τομέα της κοινωνικής πολιτικής. Πάντως, τα δεδομένα αυτά πληρούν τα διεθνή πρότυπα για επίσημες στατιστικές. Στον τομέα της κοινωνικής πολιτικής, ωστόσο, υπάρχουν πολύ περισσότερα δεδομένα εγγεγραμμένα και χρησιμοποιούμενα, όπως στο Self-Reliance Matrix (ZRM), που σχεδιάστηκε από το Διοικητικό Συμβούλιο Υγείας του Άμστερνταμ και που

χρησιμοποιείται σε πολλές μεγάλες πόλεις για τη βαθμολογία των χαρακτηριστικών των πολιτών στο σύστημα πρόνοιας (13 τομείς της καθημερινής ζωής). Αυτές οι βαθμολογίες ποικίλλουν από «έχει οξέα προβλήματα» έως «είναι απολύτως αυτοδύναμος». Είναι ένα μέσο για την υποστήριξη των πολιτών, αλλά δεν είναι επαρκές μέσο συγκέντρωσης έγκυρων και αξιόπιστων δεδομένων.

7.2 ΔΙΑΤΗΡΗΣΗ ΤΟΥ ΨΗΦΙΑΚΟΥ ΑΠΟΡΡΗΤΟΥ ΚΑΤΑ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΣΥΜΜΕΤΟΧΗ

Η εφαρμογή του Γενικού Κανονισμού περί Προστασίας των Προσωπικών Δεδομένων (GDPR) είναι μια μεγάλη πρόκληση, την οποία όμως μπορούμε να δούμε ως μια ευκαιρία να σχεδιαστούν εκ νέου οι μέθοδοι και τα συστήματα, που χρησιμοποιούνται για τη συλλογή και επεξεργασία των προσωπικών δεδομένων. Ένας τομέας στον οποίο δεν έχει γίνει αρκετή μελέτη είναι η συλλογή και η χρήση προσωπικών δεδομένων με σκοπό τη δημιουργία συστημάτων Ψηφιακής Συμμετοχής (e-Participation). Οι σύγχρονες εκδόσεις τέτοιων συστημάτων είναι κοινωνικό - τεχνικά συστήματα βασισμένα στα ταχέως αυξανόμενα σε χρήση μέσα μαζικής διαδικτύωσης, τα οποία μπορούν να χρησιμοποιηθούν ως πολύτιμα εργαλεία, που θα παρέχουν απαντήσεις σε ζητήματα που αφορούν την κοινωνική πολιτική.

Από τη δημιουργία της, η σύγχρονη κοινωνία βασίζεται στα δεδομένα. Αυτά έχουν μεγάλη αξία και η διαχείρισή τους είναι σημαντική για την οικονομία. (Spiekermann, S., 2015:161-167). Παράλληλα, ο έλεγχος αυτός των δεδομένων δημιουργεί συγκρούσεις και παρουσιάζει απειλές προς την ιδιωτικότητα, τα προσωπικά δικαιώματα και προσωπικά δεδομένα (Acquisti, A., Gritzalis, S., Lambrinoudakis, C., 2007). Τέτοιοι κίνδυνοι παρουσιάζονται λόγω της ύπαρξης του ανθρώπινου παράγοντα στο

σύστημα (Lash, S., Szerszynski, B., Wynne, B., 1996), διότι αυτές τις πληροφορίες μπορούν να τις εκμεταλλευτούν κυβερνήσεις, επιχειρήσεις ή ακόμα οργανώσεις και ιδιώτες.

Το Διαδίκτυο, η καινοτόμος αυτή τεχνολογία, είναι το θεμέλιο πάνω στο οποίο έχει χτιστεί ένας νέος τρόπος επικοινωνίας μεταξύ κοινωνικών ομάδων αλλά στο πλαίσιο της ιδιωτικής ζωής. Η εκθετική αύξηση των χρηστών του διαδικτύου και η πληθώρα και η ποικιλία των καινοτόμων υπηρεσιών που στηρίζονται σε αυτό, κυρίως των μέσων κοινωνικής δικτύωσης, έχουν σταδιακά οδηγήσει στο αποτέλεσμα να γίνουν αυτές οι υπηρεσίες κοινώς αποδεκτές στη δημόσια και στην ιδιωτική ζωή. Όλοι αυτοί οι ψηφιακοί δίαυλοι επικοινωνίας έχουν οδηγήσει σε ένα νέο είδος αλληλεπίδρασης των ανθρώπων με την πολιτική, κάτι το ιδιαίτερα σημαντικό που βοηθάει στη σταδιακή αποκατάσταση της εμπιστοσύνης του κοινού στην πολιτική και τους θεσμούς που την εκπροσωπούν.

Σε ένα περιβάλλον ηλεκτρονικής δημοκρατίας (e-democracy), η ψηφιακή συμμετοχή (e-Participation) θα δώσει τα απαραίτητα μέσα ώστε οι κυβερνητικές αποφάσεις να προσαρμοστούν στις πραγματικές ανάγκες και προσδοκίες των πολιτών (As-Saber, S., Hossainn, K., Srivastava, A., 2007:156-178, Medaglia, R., 2012:346-360, Susha, I. 2012:373-382). Ακολούθως, η συνεχής χρήση από τον λαό των μέσων κοινωνικής δικτύωσης, μέσω έξυπνων τηλεφώνων, tablet και υπολογιστών παρουσιάζει μια τρομερή ευκαιρία για κρατικούς φορείς ώστε να συλλέγουν συχνά απόψεις, προτιμήσεις και αξιολογήσεις, κάτι το ιδιαίτερα πολύτιμο ειδικά αν λάβουμε υπόψη την ισχυρή θέληση του λαού για άμεση συμμετοχή στη διακυβέρνησή του. Πάνω από όλα, όμως, το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης είναι σημαντικά εργαλεία στη λήψη αποφάσεων κατά τον σχεδιασμό δημόσιων πολιτικών, υποστηρίζοντας νέα

μοντέλα αλληλεπίδρασης μεταξύ κυβερνήσεων, επιχειρήσεων, πολιτών και ειδικών, όπως το crowdsourcing (Diamantopoulou, V., Androutsopoulou, A., Gritzalis, S., Charalabidis,Y., 2018:1-4) και την αποτελεσματική αντιμετώπιση σύνθετων ζητημάτων στις σύγχρονες δημοκρατικές κοινωνίες.

Αν και η αλληλεπίδραση μέσω διαδικτύου και μέσων κοινωνικής δικτύωσης ανοίγει νέους δρόμους για συνεργασία, ταυτόχρονα δημιουργεί και νέους κινδύνους για την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων, καθώς συχνά οι χρήστες έχουν μηδενική ή περιορισμένη επίγνωση των κινδύνων αποκάλυψης προσωπικών δεδομένων τους. Επιπλέον, φαίνεται να εφησυχάζουν εκφράζοντας μέσω της αδράνειάς τους εμπιστοσύνη στους παρόχους υπηρεσιών που χρησιμοποιούν, στην κυβέρνηση και στη νομοθεσία, πιστεύοντας ότι θα τους προστατεύσουν από την παράνομη χρήση των προσωπικών τους δεδομένων.

Ζούμε στην εποχή της Πληροφορίας και η κοινωνία αναγνωρίζει ότι οι πληροφορίες είναι δύναμη και γνώση, αλλά, χωρίς να έχουν εξασφαλιστεί αποτελεσματικά τα δικαιώματα των προσωπικών δεδομένων, ο κόσμος προβληματίζεται με την απειλή που παρουσιάζεται για την ιδιωτική του ζωή (Beldad, A., De Jong, M., Steehoulder, M., 2011:2233-2242). Η ιδιωτικότητα δεν είναι ένα νέο κοινωνικό ζήτημα, αλλά επαναπροσδιορίστηκε και είναι θέμα στην Κοινωνία της Πληροφορίας στην οποία ζούμε, δεδομένου ότι η «κλασική» έννοια της ιδιωτικής ζωής εμπλουτίστηκε σημαντικά (Mitrou, L., 2002; Mitrou, L.,2017), ενώ το εύρος της κυμαίνεται σημαντικά και σε διάφορα κοινωνικά και πολιτικά συστήματα (Solove, D.J., 2005:477; Islam, M.B., Watson, J., Iannella, R., Geva, S., 2014).

Επιπλέον, στη μεταμοντέρνα κοινωνία μας η οριοθέτηση μεταξύ ιδιωτικού και δημοσίου τομέα έχει γίνει πιο ασαφής, καθώς οι σχέσεις μεταξύ διαφορετικών φορέων διαχείρισης πληροφοριών έχουν γίνει πολύπλοκες (Newburn, T., Jones, T., 1998; Marx, G.T., 2001:157-169). Η προστασία της ιδιωτικής ζωής έχει αναγνωριστεί ως βασική αρχή σε όλες τις σύγχρονες δημοκρατίες (Henderson, S.E., 2012:227) και έχει τεκμηριωθεί ως προϋπόθεση για τη διασφάλιση μιας βιώσιμης ανάπτυξης στην ψηφιακή μας εποχή (Acquisti, A., Gritzalis, S., Lambrinoudakis, C., 2007;Cohen, J.E., 2012:1904).

Η επιτυχής εφαρμογή του GDPR σε οποιονδήποτε οργανισμό είναι ένα δύσκολο ζήτημα που απαιτεί πολλή προσπάθεια. Ωστόσο, είναι επιτακτική ανάγκη για όλους τους οργανισμούς, δημόσιους και ιδιωτικούς, να συμμορφώνονται με τον Κανονισμό, ώστε να προστατεύονται τα προσωπικά στοιχεία που επεξεργάζονται. Στην ψηφιακή κοινωνία, όπου οι υπηρεσίες είναι εξατομικευμένες και η επικοινωνία ακαριαία, οι αποφάσεις λαμβάνονται με βάση τα αποτελέσματα της επεξεργασίας των δεδομένων και αν θέλουν να υπάρχει δικαιοσύνη και διαφάνεια, πρέπει να ενημερώνονται οι χρήστες.

Ιδιαίτερη προσοχή πρέπει να δοθεί στη νομική βάση της επεξεργασίας ιδιωτικών δεδομένων. Όταν χρειάζεται συγκατάθεση, ο χρήστης θα πρέπει να μπορεί να την αποσύρει εύκολα και ανά πάσα στιγμή. Αυτό υποχρεώνει τον υπεύθυνο επεξεργασίας δεδομένων να σταματήσει την επεξεργασία εκτός εάν υπάρχει ιδιαίτερος λόγος που τη δικαιολογεί. Τέλος, συναίνεση θεωρείται ότι ελήφθη μόνο εάν έχει δοθεί ελεύθερα σε κάτι συγκεκριμένο και ξεκάθαρο και ο χρήστης ενεργά έδειξε ότι το δέχεται (ΓΚΠΔ, άρθρο 7).

7.3 ΠΡΟΚΛΗΣΕΙΣ ΜΕΤΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR

Ο GDPR έχει μετατραπεί σε μια σημαντική πρόκληση για οργανώσεις, οι οποίες αναγκάζονται να πραγματοποιήσουν μια σειρά μετατροπών και αλλαγών στα συστήματα συλλογής πληροφοριών τους, τις επιχειρηματικές τους διαδικασίες, την κουλτούρα τους και τον συνολικό τρόπο λειτουργίας τους. Ορισμένες από αυτές τις προκλήσεις έχουν καταγραφεί από οργανισμούς, ακαδημαϊκές εταιρείες ή από Ευρωπαϊκές Εκθέσεις της Επιτροπής, που ρίχνουν φως στις ιδιαίτερες πτυχές του GDPR που φαίνονται ενοχλητικές.

Η πρώτη επίσημη έκθεση σχετικά με την εφαρμογή του GDPR παρέχεται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, (EDPB,2019) που υποδεικνύει ότι οι περισσότεροι οργανισμοί έχουν καταβάλει μεγάλη προσπάθεια για συμμόρφωση με τον GDPR αυξάνοντας τον οικονομικό προϋπολογισμό τους, που διατίθεται για την προστασία των προσωπικών τους δεδομένων (30–50%), αυξάνοντας το διατιθέμενο προσωπικό, ενώ οι αρχές από 31 κράτη μέλη έχουν αντιμετωπίσει συνολικά πάνω από 206.326 νομικές υποθέσεις που σχετίζονται με καταγγελίες, παραβιάσεις δεδομένων κ.λ.π. Μια αναφορά του ISACA (ISACA, 2018) παρουσιάζει έρευνα που δείχνει ότι περίπου το 65% των οργανισμών ανέφεραν ότι δεν ήταν έτοιμοι να συμμορφωθούν με τους όρους του GDPR τον Μάϊο του 2018. Η ίδια η έκθεση επεξεργάζεται τεχνικά, ρυθμιστικά και νομοθετικά εργαλεία που θα πρέπει να εφαρμοστούν για να βοηθήσουν τους οργανισμούς στις προσπάθειές τους για να συμμορφωθούν.

Στην ίδια κατεύθυνση, η Thomson Reuters (Thomson Reuters, 2019) αναφέρει ότι οι οργανισμοί δεν είναι ακόμη έτοιμοι όσον αφορά τον GDPR, πολλοί από αυτούς γνωρίζουν ελάχιστα για τον κανονισμό και δεν γνωρίζουν ακόμη πλήρως τον πιθανό αντίκτυπο του GDPR. Σε μια έρευνα

(IAAP,2018) που διεξήχθη μεταξύ εμπειρογνωμόνων σε θέματα προσωπικών δεδομένων και απορρήτου, που δημοσιεύτηκε από την International Association of Privacy Professionals (IAPP) το 2019, αναφέρθηκε ότι λιγότερο από το 50% των ερωτηθέντων ανέφεραν ότι συμμορφώνονται πλήρως με τον GDPR. Είναι ενδιαφέρον ότι σχεδόν το 20% των επαγγελματιών απορρήτου που συμμετείχαν υποστηρίζουν ότι η πλήρης συμμόρφωση με τον GDPR είναι πραγματικά αδύνατη.

ΚΕΦΑΛΑΙΟ 8: ΣΥΓΚΡΙΣΗ ΤΩΝ EU GDPR ΚΑΙ ΤΩΝ APEC CBPR

Αυτή η ενότητα εξετάζει τα δύο μεγάλα διεθνή συστήματα μεταφοράς δεδομένων που υπάρχουν σήμερα, το μοντέλο της Ευρωπαϊκής Ένωσης (Ε.Ε.), που ουσιαστικά είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), και το μοντέλο της Οικονομικής Συνεργασίας Ασίας-Ειρηνικού (APEC),δηλαδή το σύστημα κανόνων CBPR.

Τα IoT (Internet of Things) δεδομένα, που φαινομενικά σχετίζονται με αντικείμενα, π.χ. με προϊόντα και υπηρεσίες, στην πραγματικότητα επηρεάζουν τα άτομα και το δικαίωμά τους στην προστασία των δεδομένων και της ιδιωτικότητάς τους και εγείρουν ζητήματα συμμόρφωσης για τις επιχειρήσεις σε σχέση με τις διεθνείς ροές δεδομένων. Ο GDPR ρυθμίζει την επεξεργασία των προσωπικών δεδομένων των ατόμων, που βρίσκονται εντός της Ε.Ε., συμπεριλαμβανομένων των δεδομένων που εισέρχονται ή εξέρχονται της Ε.Ε. Ως κανονισμός της Ε.Ε., ο GDPR εφαρμόζεται απευθείας ως νόμος στα κράτη μέλη της Ε.Ε. και έχει επίσης εκτενείς εξωχώριες διατάξεις, που ισχύουν για την επεξεργασία προσωπικών δεδομένων εκτός των κρατών-μελών της Ε.Ε., ανεξάρτητα από τον τόπο σύστασης και της γεωγραφικής περιοχής λειτουργίας του υπεύθυνου επεξεργασίας ή του επεξεργαστή δεδομένων.

Από την άλλη πλευρά, η APEC CBPR είναι το άλλο σημαντικό περιφερειακό πλαίσιο, που ρυθμίζει τη μεταφορά δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών της APEC. Πρόκειται ουσιαστικά για ένα σύστημα, στο οποίο εθελοντικά συμμετέχουν χώρες με σκοπό τη διευκόλυνση μεταφοράς δεδομένων μεταξύ των χωρών-μελών, οι οποίες τηρούν κάποια στάνταρ ασφαλείας και προστασίας δεδομένων, τα οποία έχουν οριστεί από την APEC Privacy Framework. Η APEC CBPR προβάλλεται από πολλούς στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ) ως προτιμότερη

από την Ευρωπαϊκή προσέγγιση, επειδή η CBPR θεωρείται πιο ευνοϊκή για τις επιχειρήσεις από τα αντίστοιχα συστήματα βάσει του GDPR και ως εκ τούτου θεωρείται το πιο πιθανό καθεστώς να επικρατήσει. Ενώ υπάρχουν μεγάλες ομοιότητες μεταξύ της προσεγγίσεως της Ε.Ε. και της APEC ως προς την προστασία και τη διασυνοριακή μεταφορά δεδομένων, υπάρχουν επίσης και ουσιαστικές διαφορές.

Το μοντέλο της Ε.Ε. είναι το πιο διαδεδομένο μοντέλο νομοθεσίας όσον αφορά τα προσωπικά δεδομένα, με τις περισσότερες χώρες στον κόσμο να το εφαρμόζουν σε κάποιον βαθμό στην εθνική τους νομοθεσία. Αυτό ισχύει τόσο για τις αναπτυσσόμενες όσο και για τις ανεπτυγμένες χώρες. (Πλέον τα κράτη έχουν διαμορφώσει τη νομοθεσία τους σύμφωνα με την Οδηγία του 1995, προκάτοχο του ισχύοντος GDPR, που τέθηκε σε λειτουργία το 2018.) Ορισμένες χώρες προσπαθούν να ακολουθήσουν πιστά τις οδηγίες, ενώ άλλες έχουν υιοθετήσει μόνο κάποια βασικά στοιχεία . Η σημαντική εξαίρεση είναι οι ΗΠΑ, που δεν ακολούθησαν γενικά το μοντέλο της Ε.Ε. για την προστασία δεδομένων.

Η εκτός Ε.Ε. εμβέλεια του GDPR αυξάνει την επιρροή του κυρίως μέσω της οργανωτικής πρακτικής και διαδικασίας, με την οποία αντιλαμβάνονται οι εταιρείες εκτός της Ε.Ε. ότι πρέπει να συμμορφωθούν, επειδή επεξεργάζονται τα προσωπικά δεδομένα των πολιτών της Ε.Ε. Αυτό έχει προκαλέσει ανησυχίες ιδιαίτερα στις πολυεθνικές των ΗΠΑ σχετικά με το κόστος συμμόρφωσης και την ανάγκη προσαρμογής τους σε παγκόσμιο επίπεδο. Στις ΗΠΑ, η προσέγγιση της APEC, που χρησιμοποιεί το σύστημα CBPR, θεωρείται ευρέως ότι είναι το καλύτερο μοντέλο για τη διασυνοριακή μεταφορά δεδομένων, κυρίως γιατί θεωρείται λιγότερο δεσμευτικό και περιοριστικό από τον GDPR και επομένως ευνοεί περισσότερο και διευκολύνει τις διασυνοριακές ροές δεδομένων. Η APEC

είναι ένα περιφερειακό οικονομικό φόρουμ, που ιδρύθηκε το 1989 για να αξιοποιήσει την αυξανόμενη αλληλεξάρτηση Ασίας-Ειρηνικού (APEC, 2019).

Η δομή της APEC έχει βασιστεί στην Ε.Ε., καθώς είναι ένα περιφερειακό σώμα, από το οποίο ,όμως, λείπουν οι νομοθετικές εξουσίες της Ε.Ε. και οι μηχανισμοί επιβολής και διακυβέρνησης. Η APEC έχει επί του παρόντος 21 οικονομικά μέλη, που περιλαμβάνουν κυρίως χώρες της Ασίας, του Ειρηνικού, αλλά επίσης συμπεριλαμβάνονται και οι ΗΠΑ, ο Καναδάς, η Χιλή, το Μεξικό και η Ρωσία (APEC, 2019). Ο επίσημος στόχος της APEC είναι «να δημιουργήσει μεγαλύτερη ευημερία για τους ανθρώπους αυτών των περιοχών προϋποθέτοντας μια ανάπτυξη ισορροπημένη, χωρίς αποκλεισμούς, βιώσιμη, καινοτόμο και ασφαλή και με επιτάχυνση της διασυνοριακής μεταφοράς δεδομένων.

Σύμφωνα με αυτόν το στόχο, η APEC CBPR ιδρύθηκε το 2012 ως εθελοντικό περιφερειακό σχέδιο για να διευκολύνει τις διασυνοριακές ροές των δεδομένων μεταξύ των χωρών - μελών που πληρούν τα πρότυπα προστασίας δεδομένων, όπως ορίζονται από το σχέδιο. Το CBPR βασίζεται στις αρχές προστασίας δεδομένων που ορίζονται στο Πλαίσιο Προστασίας Προσωπικών Δεδομένων της APEC (Πλαίσιο). Το σύστημα του CBPR απαιτεί, για να ενταχθεί μια χώρα στο CBPR, να προσαρμοστεί πρώτα στις απαραίτητες νομοθετικές και εκτελεστικές απαιτήσεις, ώστε μια εταιρεία, που επιθυμεί να μεταφέρει δεδομένα βάσει σχεδίου, να δέχεται μια ανεξάρτητη αξιολόγηση συμμόρφωσης (“APEC Cross-Border Privacy Rules (CBPR) System, 2019). Το 2012, οι ΗΠΑ έγιναν το πρώτο έθνος που συμμετείχε στο CBPR και η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC) έγινε η πρώτη εγχώρια αρχή επιβολής. Η FTC και μερικές εταιρείες των ΗΠΑ είναι συνήγοροι αυτού του συστήματος.

8.1 ΟΜΟΙΟΤΗΤΕΣ ΚΑΙ ΔΙΑΦΟΡΕΣ

Υπάρχουν έντονες ομοιότητες μεταξύ της APEC CBPR και των διασυνοριακών μηχανισμών μεταφοράς του GDPR της Ε.Ε. Σύμφωνα με τον GDPR υπάρχει μια σειρά από εθελοντικές επιλογές για τις εταιρείες σε χώρες όπως οι ΗΠΑ, αυτό, όμως, δεν σημαίνει ότι έχουν ισοδύναμες απαιτήσεις απορρήτου και προστασίας δεδομένων με αυτές της ΕΕ.

Επιπλέον, εκτός από το γνωστό EU/US πεδίο απορρήτου (Privacy Shield), άλλοι αποδεκτοί μηχανισμοί περιλαμβάνουν τη χρήση των τυπικών συμβατικών ρητρών, εγκεκριμένους Κώδικες Δεοντολογίας και πιστοποίηση σύμφωνα με τον GDPR. Αυτό έρχεται σε αντίθεση με την APEC, που έχει ένα μόνο εθελοντικό πρόγραμμα, το CBPR, για τα μέλη του. Οι περισσότεροι από τους μηχανισμούς μεταφοράς έχουν ομοιότητες, αλλά το CBPR είναι παρόμοιο σε προσέγγιση με την Privacy Shield στο ότι το CBPR απαιτεί αποδοχή σε επίπεδο χώρας, ακολουθούμενη από μια ανεξάρτητη πιστοποιημένη διαδικασία για τον μεμονωμένο οργανισμό, που επιθυμεί να ενταχθεί στο πρόγραμμα (Clare Sullivan, 2019).

Επίσης, σε αντίθεση με την APEC CBPR, ο GDPR αποτελεί μέρος μιας σχετικά ολοκληρωμένης σειράς κανονισμών, που προορίζονται να αντιμετωπίσουν ένα ευρύ φάσμα θεμάτων, που σχετίζονται με την ψηφιακή εποχή. Το πακέτο μεταρρύθμισης της προστασίας δεδομένων, που τέθηκε σε ισχύ το 2018 αποτελείται από τον GDPR και την Οδηγία για την Προστασία Δεδομένων για την Αστυνομία και την ποινική Δικαιοσύνη (DPDPC). Αυτό το πακέτο μεταρρυθμίσεων όχι μόνο ενημερώνει και αντικαθιστά τον Οδηγό προστασίας των δεδομένων του 1995, αλλά μεταρρυθμίζει και την απόφαση του 2008 για τον τομέα της αστυνομίας και της ποινικής δικαιοσύνης, που έχει σχεδιαστεί για τη διευκόλυνση της

διασυνοριακής συνεργασίας για την αποτελεσματικότερη καταπολέμηση του εγκλήματος και της τρομοκρατίας (APEC, 2019).

Ένα βασικό μέρος αυτού του πακέτου μεταρρυθμίσεων είναι ο κανονισμός σχετικά με τον σεβασμό της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων, που θα ισχύουν στις Ηλεκτρονικές Επικοινωνίες. Αν και αρχικά είχε προγραμματιστεί να τεθεί σε ισχύ ταυτόχρονα με τον GDPR το 2018, ο νέος κανονισμός ιδιωτικότητας δεν επρόκειτο να γίνει νόμος στην Ε.Ε. μέχρι το 2019. Ο προτεινόμενος κανονισμός ιδιωτικότητας ενημερώνει και αντικαθιστά την τρέχουσα οδηγία για την προστασία της ιδιωτικής ζωής όσον αφορά τις ψηφιακές επικοινωνίες. Αλλάζει ουσιαστικά και επεκτείνει την ισχύουσα οδηγία,ώστε να εφαρμόζεται και στις υπηρεσίες over-the-top (OTT), όπως το WhatsApp, το Facebook, το Messenger και το Skype, με τα μετα-δεδομένα (metadata), που σχετίζονται με τις ψηφιακές επικοινωνίες και τις επικοινωνίες IoT.

Το καθεστώς APEC δεν ισχύει αποκλειστικά για τις ψηφιακές επικοινωνίες. Για αυτό μια καλύτερη ιδέα για την Ε.Ε. είναι να εφαρμόσει τις απαιτήσεις της για την προστασία δεδομένων στο IoT μέσω του GDPR, αντί να εντάξει τα δεδομένα IoT σε έναν νέο κανονισμό, τον ePrivacy. Ωστόσο, η συνολική παρατήρηση σχετικά με αυτήν τη συζήτηση είναι ότι σε σύγκριση με τους ισχύοντες κανονισμούς στην Ε.Ε., η προσέγγιση της APEC είναι πολύ λιγότερο ολοκληρωμένη.

Η νομική βάση της ευρωπαϊκής προσέγγισης είναι ουσιαστικά διαφορετική από αυτή του συστήματος APEC. Οι κανονισμοί της Ε.Ε. βασίζονται και στο δικαίωμα εμπιστοσύνης στις επικοινωνίες. Ενώ οι αρχές της προστασίας των δεδομένων της APEC είναι σε γενικές γραμμές παρόμοιες με του GDPR, η πρώτη δεν βασίζεται στα θεμελιώδη ανθρώπινα δικαιώματα, ούτε στηρίζεται στη νομολογία με τον ίδιο τρόπο, ούτε στον ίδιο βαθμό όπως οι

κανονισμοί της Ε.Ε. Στο σύνολό της η APEC τείνει να στοχεύει περισσότερο στη διευκόλυνση της μεταφοράς δεδομένων βάσει κάποιων κοινώς αποδεκτών παραμέτρων για την προστασία τους. Είναι εμφανές ότι ένας από τους καθορισμένους στόχους της APEC CBPR είναι να προωθηθεί «ένα πλαίσιο πολιτικής, που έχει σχεδιαστεί με σκοπό να διασφαλίσει τη συνεχή ελεύθερη ροή των προσωπικών πληροφοριών διασυνοριακά, αλλά με ένα αξιόλογο επίπεδο προστασίας, μεριμνώντας για το απόρρητο και την ασφάλεια των προσωπικών πληροφοριών» (Clare Sullivan, 2019).

Η ακόλουθη σύγκριση εστιάζει στις βασικές διαφορές μεταξύ των διατάξεων του GDPR για το σύστημα μεταφοράς δεδομένων της Ε.Ε. και του πλαισίου κανονισμών CBPR για την APEC .

- Το πλαίσιο APEC και ο GDPR ισχύουν για την παραβίαση προσωπικών δεδομένων στον ιδιωτικό και δημόσιο τομέα. Ένας δεδηλωμένος στόχος του GDPR είναι η ενημέρωση για την προστασία δεδομένων στη σύγχρονη εποχή που περιλαμβάνει τα IoT (Internet of Things) , Big Data, και AI (Artificial Intelligence). Από την άλλη πλευρά, το πλαίσιο APEC, το οποίο ενημερώθηκε το 2015, αναφέρεται στην τεχνολογική ανάπτυξη και τον αντίκτυπο της κινητής τεχνολογίας, αλλά δεν εξετάζει συγκεκριμένα τις πτυχές που καλύπτονται από τον GDPR.

- Τόσο το μοντέλο APEC όσο και το μοντέλο της Ε.Ε. στοχεύουν στη διευκόλυνση των ροών δεδομένων και την προστασία των προσωπικών δεδομένων, που ορίζονται ουσιαστικά με τους ίδιους όρους, τόσο σύμφωνα με τον GDPR όσο και με το πλαίσιο APEC. Η διευκόλυνση των διασυνοριακών ροών δεδομένων και η ταυτόχρονη προστασία τους είναι ιδιαίτερα σημαντική για τα IoT δεδομένα. Κάθε σύστημα έχει διαφορετική νομοθετική βάση. Ο GDPR αφορά την προστασία των θεμελιωδών

δικαιωμάτων και των φυσικών προσώπων, ιδίως το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα, ενώ η APEC έχει σχεδιαστεί για να διευκολύνει τις διασυνοριακές ροές δεδομένων, σύμφωνα με τον πρωταρχικό στόχο της ενθάρρυνσης του εμπορίου μεταξύ των μελών της. Αυτή η διαφορετική εννοιολογική βάση αντικατοπτρίζεται στο πλαίσιο του κανονισμού APEC, που θεσπίζει την προστασία των προσωπικών δεδομένων κυρίως σε περιπτώσεις, που υπάρχει κίνδυνος οικονομικής ή σωματικής βλάβης ενός ατόμου, ενώ ο GDPR βασίζεται στην προστασία των θεμελιωδών ανθρωπίνων δικαιωμάτων.

- Οι περισσότερες από τις CBPR απαιτήσεις εκφράζονται με όρους ό,τι είναι «λογικό» και ό,τι είναι «κατάλληλο» (όροι που χρησιμοποιούνται επίσης ευρέως στον GDPR), και εξαρτώνται από τον κίνδυνο και το είδος της βλάβης, άρα υπάρχει περιορισμένη καθοδήγηση από το πλαίσιο CBPR προς τις εταιρείες, κυρίως μέσω των κριτηρίων αξιολόγησης και των απαιτήσεών τους ως προς τους παράγοντες που πρέπει να λαμβάνονται υπόψιν, όταν υφίσταται κίνδυνος. Αυτή η προσέγγιση επιτρέπει μια ευελιξία, αλλά μπορεί επίσης να οδηγεί σε αβεβαιότητα και έλλειψη σαφήνειας ως προς το επίπεδο προστασίας με τα δοθέντα προσωπικά στοιχεία .

- Η μελέτη των βασικών στοιχείων του GDPR και του CBPR, όπως ισχύουν για την επεξεργασία δεδομένων IoT, αποκαλύπτει ξεκάθαρα ότι το μοντέλο APEC δεν είναι τόσο περιεκτικό, ούτε τόσο λεπτομερές όσο το GDPR.

- Σε αντίθεση με το Πλαίσιο, που αποτελεί το ελάχιστο πρότυπο προστασίας δεδομένων, στο οποίο οι οργανισμοί απαιτείται να είναι πιστοποιημένοι για CBPR, ο GDPR είναι σχετικά πιο λεπτομερής, και σαφής,

ως προς τις συγκεκριμένες απαιτήσεις και αυτές οι απαιτήσεις ισχύουν άμεσα ως νόμος (Clare Sullivan, 2019).

8.2 ΣΥΜΠΕΡΑΣΜΑΤΑ

Η ανασκόπηση των μοντέλων της Ε.Ε. και της APEC σε σχέση με τις πτυχές, που σχετίζονται με την επεξεργασία των δεδομένων IoT, αποκαλύπτει ότι, ενώ υπάρχουν ομοιότητες στην ορολογία και στη γενική προσέγγιση, οι βασικοί στόχοι και τα πρότυπα διαφέρουν. Η σύγκριση δείχνει ότι το Πλαίσιο της APEC δεν έχει την ακρίβεια, τη σαφήνεια και την καθοδήγηση, που απαιτούνται για ένα πρότυπο αυτής της φύσεως και ότι, γενικά, δεν πληροί τις προϋποθέσεις που ορίζει ο GDPR. Το CBPR δεν είναι σύμφωνο με αρκετές από τις ευρέως αποδεκτές καλές πρακτικές, όπως, για παράδειγμα, δεν αναγκάζει τις εταιρείες να ορίζουν ειδικούς-υπεύθυνους προστασίας δεδομένων (Clare Sullivan, 2019).

Η δημιουργία του IoT υπογραμμίζει την ανάγκη για αποτελεσματικούς μηχανισμούς διευκόλυνσης των διεθνών ροών δεδομένων, ενώ, παράλληλα, θα προστατεύονται τα προσωπικά δεδομένα. Αν και το IoT προσφέρει πολλά οφέλη για τα άτομα και τις επιχειρήσεις, υπάρχουν σαφώς ατομικοί κίνδυνοι απορρήτου, ειδικά όταν τα δεδομένα μεταφέρονται εκτός συνόρων. Δεδομένης της ανησυχίας των εταιρειών για την ανάγκη συμμόρφωσης κατά την επεξεργασία των δεδομένων, το θέμα που διερευνήθηκε εδώ είναι ποιο σύστημα είναι περισσότερο αποτελεσματικό να επιτυγχάνει ουσιαστικά αυτή την ισορροπία στο πλαίσιο της επεξεργασίας δεδομένων IoT. Όπως προαναφέρθηκε, υπάρχουν κάποιες ευρείες ομοιότητες, αλλά υπάρχουν επίσης αξιοσημείωτες διαφορές στην εννοιολογική βάση και στους στόχους, στην καθοδήγηση και στις απαιτήσεις. Υπάρχει σημαντική διαφορά ανάμεσα στο γενικό πρότυπο προστασίας δεδομένων (GDPR) και στην προστασία που

προσφέρει το CBPR . Το CBPR είναι ένας μηχανισμός που διευκολύνει το εμπόριο εντός της περιοχής της APEC. Η Ιαπωνία, για παράδειγμα, επιτρέπει αυτόματα διασυνοριακές μεταφορές από εταιρείες που έχουν έγκριση CBPR, ενώ οι άλλες εταιρείες πρέπει πρώτα να λάβουν συγκατάθεση σύμφωνα με τον νόμο για την προστασία των προσωπικών πληροφοριών (Clare Sullivan, 2019).

ΣΥΜΠΕΡΑΣΜΑΤΑ

ΠΩΣ Ο GDPR ΘΑ ΑΛΛΑΞΕΙ ΤΟΝ ΚΟΣΜΟ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ε.Ε. (GDPR) από τις 24 Μαΐου του 2018 ισχύει και εφαρμόζεται στις δραστηριότητες επεξεργασίας προσωπικών δεδομένων που προέρχονται από χρήστες στην επικράτεια της Ευρωπαϊκής Ένωσης. Η παράβασή του θα τιμωρείται με κυρώσεις της τάξεως του 4% των παγκόσμιων εσόδων της εταιρείας ή 100 εκατ. Ευρώ, ό,τι είναι μεγαλύτερο. Όλες οι Αρχές Προστασίας Δεδομένων (DPA) θα πρέπει να επιβάλλουν αυτές τις κυρώσεις και είναι εξοπλισμένες με ευρεία σειρά εργαλείων και εξουσιών. Οι αποφάσεις πλειοψηφίας από μια νεοσύστατη Ευρωπαϊκή Προστασία Δεδομένων μπορούν να αναγκάσουν οποιαδήποτε DPA των κρατών μελών να υιοθετήσει, να αλλάξει ή να αποσύρει ένα συγκεκριμένο μέτρο. Από τις 24 Μαΐου 2018 θα σταματήσει να υφίσταται η κατακερματισμένη ψηφιακή αγορά και η έλλειψη ελέγχου στον τομέα των διατάξεων και προστασίας δεδομένων. Θα υπάρχει ένας ενιαίος και άμεσα εφαρμοστέος νόμος για την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση, που αντικαθιστά σχεδόν όλες τις υφιστάμενες διατάξεις των κρατών μελών και η οποία θα πρέπει να εφαρμόζεται από επιχειρήσεις, ιδιώτες, δικαστήρια και αρχές ,ώστε να μην υπάρχει ανάγκη

καταφυγής στο εθνικό δίκαιο. Αυτοί που προσπαθούν να δημιουργήσουν μια διαφορετική αντίληψη αρνούμενοι αυτό το γεγονός, βάζουν σε κίνδυνο όλους όσοι πρέπει να προετοιμαστούν για αυτόν τον νέο νόμο.

Υπάρχουν κάποιοι που λένε ότι ο GDPR δεν θα δημιουργήσει περισσότερη εναρμόνιση αλλά, αντίθετα, θα δημιουργήσει ακόμη περισσότερες εθνικές διαφορές από πριν. Το βασικό τους επιχείρημα είναι ότι ο GDPR έχει πολλές διατάξεις όπου γίνεται αναφορά στη νομοθεσία των κρατών μελών και ότι αυτός ο κανονισμός θα ήταν στην πραγματικότητα περισσότερο μία οδηγία. Αυτή η άποψη αγνοεί το γεγονός ότι η αλλαγή από οδηγία σε κανονισμό αποτελεί από μόνη της μια επαναστατική αλλαγή. Αντί τα κράτη μέλη να πρέπει να μεταφέρουν κάθε διάταξη σύμφωνα με το εθνικό δίκαιο με ιδιαίτερη προσοχή, ο GDPR ρυθμίζει το σύνολο των περιπτώσεων άμεσα και αφήνει ιδιαίτερες περιπτώσεις και τις αντίστοιχες εξουσίες στα κράτη μέλη, που πρέπει στη συνέχεια να αιτιολογούν πάντα οποιαδήποτε απόκλιση από τον στόχο του εναρμονισμένου νομικού πλαισίου. Είναι σαφές ότι θα υπάρξουν τομείς όπου τα κράτη μέλη εξακολουθούν να διατηρούν τις αρμοδιότητές τους, για παράδειγμα σχετικά με τους νόμους για τα μέσα ενημέρωσης, τον τύπο ή την εθνική ασφάλεια και άμυνα. Και είναι φυσικό ο GDPR να μην ορίζει όλες τις δυνατότητες για συγκεκριμένες δραστηριότητες επεξεργασίας δεδομένων στον δημόσιο τομέα για τις οποίες το εθνικό δίκαιο, όπως συμβαίνει σήμερα, θα παρέχει τη νομική βάση για τη λύση τέτοιων προβλημάτων.

Είναι θέμα υψίστης σημασίας να κατανοήσουμε πώς το GDPR θα αλλάξει όχι μόνο την κατάσταση στην Ευρώπη αλλά και σε ολόκληρο τον κόσμο. Ήδη η συμφωνία μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου τον Δεκέμβριο του 2015 έχει αντίκτυπο στην αγορά και τις επιχειρηματικές στρατηγικές. Πολλές εταιρείες έχουν αποφασίσει να

θέσουν τη συμμόρφωσή τους με τον GDPR ως έναν από τους πρωταρχικούς στόχους τους. Ορισμένες ισχυρές οργανώσεις αλλάζουν ακόμη και τις στρατηγικές τους για να γίνουν πρωτοπόρες σχετικά με προϊόντα και υπηρεσίες φιλικά προς την προστασία δεδομένων. Το νέο μότο όλων των υπηρεσιών που προέρχονται από την Ευρώπη θα γίνει: ιδιωτικότητα, ασφάλεια και προστασία δεδομένων. Οι αρχές και οι κανόνες προστασίας δεδομένων δεν θα ισχύουν μόνο σε θεωρητικό επίπεδο, αλλά θα επιβάλλονται σταθερά σε ολόκληρη την ευρωπαϊκή επικράτεια μέσω βαρέων κυρώσεων, αλλά και θα χρησιμεύσουν ως ένα παγκόσμιο πρότυπο για κάθε νέα καινοτομία, για την εμπιστοσύνη των καταναλωτών στις ψηφιακές τεχνολογίες και θα φέρουν μία νέα ανάπτυξη.

Όσον αφορά τις ουσιαστικές διατάξεις, ο GDPR θα επιφέρει περισσότερη ασφάλεια και συνοχή στα ήδη υπάρχοντα 28 διαφορετικά δικαστικά και νομικά πλαίσια και κουλτούρες ξεκαθαρίζοντας το νομικό περιβάλλον. Στην εποχή μας, που απλώς καμία εταιρεία δεν έχει την πολυτέλεια να μην είναι παρούσα στην ψηφιακή σφαίρα και να μην παρέχει τις υπηρεσίες της μέσω διαδικτύου, το πρότερο πολύπλοκο σύστημα απλώς δημιουργούσε τεράστια γραφειοκρατία και ιδιαίτερη αβεβαιότητα. Η μεταβολή σε ένα νέο ενιαίο νομικό πλαίσιο, που περιλαμβάνει ίσους όρους ανταγωνισμού για όλες τις εταιρείες στην ευρωπαϊκή αγορά, είναι εξαιρετικά θετική και για τις επιχειρήσεις και για τους καταναλωτές.

Αλλά αυτό είναι μόνο η αρχή. Η αντικατάσταση των προηγούμενων ειδοποιήσεων στους παραβάτες με μία αυστηρή εφαρμογή των διατάξεων περί προσωπικών δεδομένων, θα καθοδηγήσει τις εταιρείες στη σωστή εφαρμογή δραστικά. Η εισαγωγή πολλών διατάξεων για περισσότερη διαφάνεια και οι απλές πολιτικές πληροφόρησης είναι υψίστης σημασίας προκειμένου να δοθεί πίσω ο έλεγχος στους καταναλωτές και να κάνουν τη

συγκατάθεσή τους ουσιαστική και πάλι. Νέες καινοτόμες ιδέες, όπως το δικαίωμα στη μεταφορά δεδομένων, τυποποιημένο μοντέλο προστασίας προσωπικών δεδομένων και ιδιωτικότητας σε όλες τις υπηρεσίες δημιουργούν νέες ευκαιρίες για καινοτομία και ανταγωνισμό στην κατεύθυνση της προστασίας δεδομένων δημιουργώντας προϊόντα και υπηρεσίες φιλικές προς τα δικαιώματα του καταναλωτή. Με τις νέες διατάξεις αντιμετώπισης επικίνδυνων διαρροών, που απαιτούν ταχείες ειδοποιήσεις σε περίπτωση παραβίασης, ανεξάρτητες αξιολογήσεις των μεθόδων προστασίας των δεδομένων και ορισμό υπευθύνων ψηφιακής ασφάλειας, μπορούν να προστατευτούν αποτελεσματικά τα προσωπικά δεδομένα στην ψηφιακή ζωή, αλλά ταυτόχρονα και οι ίδιες οι εταιρείες να έχουν ένα ξεκάθαρο και λογικό σύστημα στο οποίο πρέπει να συμμορφωθούν.

Προκειμένου να τηρηθεί η υπόσχεση της Ε.Ε. για την προστασία των δεδομένων, το Δικαστήριο της Δικαιοσύνης της Ε.Ε. κατέστησε πρόσφατα πολύ σαφές ότι δεν υπάρχει τρόπος να παρακάμψει κανείς την απαίτηση για υψηλά επίπεδα προστασίας των προσωπικών δεδομένων στην Ε.Ε.. Επομένως, ο GDPR είναι η λογική συνέχεια των ήδη υπαρχουσών αποφάσεων των Ευρωπαϊκών Δικαστηρίων, ιδίως για υποθέσεις (Google κατά Ισπανίας) σχετικά με το «δικαίωμα στη λήθη» και (Facebook v Ιρλανδίας) περί των ασφαλών λιμανιών. Η ξεκάθαρη απόφαση του Δικαστηρίου περί προστασίας των διεθνώς μεταφερόμενων δεδομένων είναι αποτέλεσμα των υποκείμενων προβλημάτων που προέκυψαν κατά τη διάρκεια της αυξανόμενης οικονομίας του διαδικτύου στη Silicon Valley και αλλού την τελευταία δεκαετία. Ο GDPR τώρα θέτει ένα πρότυπο που πρέπει να εκληφθεί ως σαφής δήλωση από τη παγκόσμια αγορά.

Κανένας υπεύθυνος επεξεργασίας δεδομένων δεν θα μπορεί να το αγνοήσει και άλλες κυβερνήσεις θα βρίσκονται υπό πίεση να αυξήσουν τα πρότυπα προστασίας των δεδομένων τους προκειμένου να τους επιτραπεί η πρόσβαση των τοπικών εταιρειών τους στην ψηφιακή ενιαία αγορά της Ευρωπαϊκής Ένωσης, η οποία είναι η μεγαλύτερη αγορά στον πλανήτη. Οι επιπτώσεις αυτού μπορεί να φανούν ήδη σήμερα, όπου ορισμένες χώρες, όπως η Ιαπωνία, συζητούν την εισαγωγή παρόμοιων διατάξεων με αυτές που ορίζονται στον GDPR και οι επιχειρήσεις του Ηνωμένου Βασιλείου κάνουν ό,τι καλύτερο μπορούν ώστε να βεβαιωθούν ότι ο GDPR θα εφαρμοστεί πλήρως ακόμη και μετά το Brexit. Κατά την αναθεώρηση της Σύμβασης του Συμβουλίου της Ευρώπης 108, ο GDPR θα αφήσει το αποτύπωμά του και σε γειτονικές χώρες της Ε.Ε. και πιθανώς ακόμα και πιο μακριά. Σε αντίθεση με τη θεωρία τρόμου, σύμφωνα με την οποία κάποιοι υποστηρίζουν ότι η Ευρώπη θα είναι ένα φρούριο το οποίο θα αποκοπεί λόγω της εξάρτησής του από τις αμερικάνικες εταιρείες, ο GDPR θα γίνει ένα διεθνές και αξιόπιστο νομοθετικό μοντέλο και για τις υπόλοιπες χώρες στον πλανήτη.

Το νεοσυσταθέν Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων θα αναγκάσει επιτέλους τις Αρχές Προστασίας Δεδομένων στην Ευρώπη να επιτύχουν μια συνεπή ερμηνεία και επιβολή του GDPR στην ενιαία αγορά. Όταν μία Αρχή Προστασίας Δεδομένων εντοπίσει πρόβλημα στην εφαρμογή κάποιου από τους κανονισμούς σε μία οργάνωση, το αναφέρει στο Συμβούλιο και, αν ο οργανισμός δεν συμμορφωθεί, το Συμβούλιο δια πλειοψηφίας αποφασίζει. Δυνατότητα προσφυγής κατά της απόφασης του Συμβουλίου θα κρίνεται από το εθνικό ή το Ευρωπαϊκό Δικαστήριο ανάλογα με την περίπτωση. Αυτή η διαδικασία θα βελτιώσει σημαντικά την αίσθηση δικαίου και τη συνοχή στον τομέα της νομοθεσίας περί προστασίας δεδομένων.

Το Συμβούλιο και τα δικαστήρια θα έχουν το καθήκον να προσαρμόσουν την εφαρμογή του GDPR σε κάθε νέα εξέλιξη στην τεχνολογία, στην αγορά και στις μεταποιητικές δραστηριότητες. Με αυτό το νέο πλαίσιο ο Γενικός Κανονισμός Προστασίας των Δεδομένων θα χρησιμεύσει ως πρότυπο και για άλλους τομείς πολιτικής, όπου οι συνέπειες της παγκοσμιοποίησης και της ψηφιοποίησης απαιτούν μια νέα ρυθμιστική προσέγγιση προκειμένου να διαφυλαχθούν οι αξίες και τα πρότυπα. Έτσι, θα βγει η Ευρωπαϊκή Ένωση από την αδράνεια και θα δείξει ότι είναι δυνατή η επίτευξη κοινής δράσης μέσω μιας δημοκρατικής διαδικασίας στη βάση υψηλών προτύπων για τα δικαιώματα των πολιτών και των καταναλωτών, καθώς και μια ανταγωνιστική και καινοτόμος ενιαία αγορά (Jan Philipp Albrecht, 2016).

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΠΔ Αρχή Προστασίας Δεδομένων

ΑΠΔΠΧ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΑΦΜ Αριθμός φορολογικού μητρώου

Ε.Ε. Ευρωπαϊκή Ένωση

ΕΕΠΔ Ευρωπαϊκή Εποπτεία Προστασίας Δεδομένων

ΕΟΧ Ευρωπαϊκός Οικονομικός Χώρος

Η.Π.Α Ηνωμένες Πολιτείες Αμερικής

ΚΚΒΠ Κλειστό Κύκλωμα Βιντεοπαρακολούθησης

ΟΤΕ Οργανισμός Τηλεπικοινωνιών Ελλάδος

ΠΟΥ Παγκόσμιος Οργανισμός Υγείας

ΤΠΕ Τεχνολογίες Πληροφορικής και Επικοινωνίας

ΥΠΔ Υπεύθυνος Προστασίας Δεδομένων

APEC Asia – Pacific Economic Cooperation

BRP Brand Risk Protection

CBPR Cross Border Privacy Rules System

CCTV Closed – circuit television

CIS Center of Internet Security

DPO Data Protection Officer

DPIA Data Protection Impact Assessment

EDPB Ευρωπαϊκή Προστασία Δεδομένων του διοικητικού συμβουλίου

FTC Federal Trade Commission

GDPR General Data Privacy Regulation

IAPP International Association of Privacy Professionals

IP Inernet Protocol

IoT Internet of Things

OTT over-the-top

PPIA Public Policy International Affairs program

RQ Research Question

SAR Subject access requests

SRM Self-Reliance Matrix

VNG Διευθυντής Ένωσης Ολλανδικών Δήμων

WHO World Health Organization

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

ΕΛΛΗΝΟΓΛΩΣΣΕΣ

Αιτιολογική Σκέψη 50, 2018, http://gdpr-text.com/el/, Ανάκτηση 5/2/2022

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ, 2020, *Ασφάλεια Επεξεργασίας*, https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/asfaleia_epexergasias/ , Ανάκτηση 15/1/2022

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ, 2020, *Πολιτική Ασφαλείας, Σχέδιο Ασφαλείας και Σχέδιο Ανάκαμψης από Καταστροφές*, https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/sxedioanakamsisasfaleiaproswpikwnsxedioanakamsisasfaleiaproswpikwn/ , Ανάκτηση 16/1/2022

ΑΠΔΠΧ, *Χρηματοπιστωτικά, Σημαντικά αρχεία* http://www.dpa.gr/portal/page?_pageid=33,124336&_dad=portal&_schema=PORTAL/ , Ανάκτηση 16/1/2022

Ασφάλεια Πληροφοριακών Συστημάτων, https://el.wikipedia.org/wiki, Ανάκτηση 20/01/2022

Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) ,2018, https://pofee.gr/images/books/GDPR-pofee-april2018.pdf/, Ανάκτηση 15/1/2022

Ένας χρόνος εφαρμογής του GDPR. Τι έγινε, τι θα γίνει, τι πρέπει να γίνει, 2019, http://www.epixeiro.gr/article/126595/, Ανάκτηση 28/1/2022

Σύνδεσμος Επιχειρήσεων και Βιομηχανιών, 2019, «*Ψηφιακή και Τεχνολογική Ωριμότητα Οικονομίας και Επιχειρήσεων»,* Παρατηρητήριο Ψηφιακού Μετασχηματισμού, 1η Ετήσια Έκδοση, Ιούλιος, Αθήνα

Παρασκευάς Μ., Ασημακόπουλος Γ., Τριανταφύλλου Β., 2017, «*Κοινωνία της Πληροφορίας: υποδομές, υπηρεσίες και επιπτώσεις*», Εκδόσεις Κάλλιπος, Αθήνα

Πομπόρτσης Α., 2017, «*Εισαγωγή στην Ηλεκτρονική Διακυβέρνηση (E – Government): ο μετασχηματισμός* των λειτουργιών και *υπηρεσιών της δημόσιας διοίκησης στην ψηφιακή εποχή*», Εκδόσεις Τζιόλας, Δεκέμβριος, Αθήνα

Πώς θα επηρεάσει το GDPR το Facebook, τα social media και εσάς, 2018 https://www.iefimerida.gr/news/419049/pos-tha-epireasei-gdpr-facebook-ta-alla-social-media-kai-esas/ , Ανάκτηση 28/1/2022

Σύνδεσμος Επιχειρήσεων και Βιομηχανιών, 2019, «*Ψηφιακή και Τεχνολογική Ωριμότητα Οικονομίας και Επιχειρήσεων*», Παρατηρητήριο Ψηφιακού Μετασχηματισμού, 1η Ετήσια Έκδοση, Ιούλιος, Αθήνα

Τι είναι η παραβίαση δεδομένων και τι πρέπει να κάνουμε σε περίπτωση παραβίασης δεδομένων;

https://ec.europa.eu/info/law/law-topic/data protection/reform/rules-business-andorganisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el/, Ανάκτηση 27/1/2022

Τι συνέβη με το Facebook και τη μεγαλύτερη διαρροή προσωπικών δεδομένων, 2018, https://thepressproject.gr/ti-sunebi-me-to-facebook-kai-tin-megaluteri-diarroi-prosopikon-dedomenon/, Ανάκτηση 24/01/2022

ΥπουργείοΔικαιοσύνης,2018, http://www.opengov.gr/ministryofjustice/?p=9326/, Ανάκτηση 16/1/2022

Υπουργείο Εσωτερικών, 2020, *«Κεφάλαιο 4: Κατευθυντήριες Αρχές»,* http://www.opengov.gr/digitalandbrief/?p=2147/, Ανάκτηση 20/12/2021

Υπουργείο Ψηφιακής Διακυβέρνησης, 2017, «*Βίβλος Ψηφιακού Μετασχηματισμού 2020 – 2025»*, Υπουργείο Ψηφιακής Διακυβέρνησης, Δεκέμβριος, Αθήνα

ΞΕΝΟΓΛΩΣΣΕΣ

Acquisti A., Gritzalis S., Lambrinoudakis C., di Vimercati, S., 2007, *Digital Privacy: Theory, Technologies, and Practices*; CRC Press: Boca Raton, FL, USA.

Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act). 2018 May 23. https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf/, Ανάκτηση 3/2/2022

Adequacy decisions, 2021, *European Commission*. https://ec.europa.eu/, Ανάκτηση 1/2/2022

A. K. Green, K. E. Reeder-Hayes, R. W. Corty, E. Basch, M. I.

Milowsky, S. B. Dusetzina, A. V. Bennett, and W. A. Wood, 2015, "*The project data sphere initiative: accelerating cancer research by sharing data*," The oncologist, vol. 20, no. 5, pp. 464–e20.

Andersen T (2019) *Legal experts: Gladsaxe's algorithm violates personal data law.* Version 2, IT News. Available at https://www.version2.dk/artikel/juridiske-eksperter-gladsaxes-algoritme-overtraeder-persondata-lov-1087407/, Ανάκτηση 2/2/2022

"APEC Cross-Border Privacy Rules (CBPR) System", 2019, *By applying this commonly agreed-upon baseline set of rules, the CBPR system bridges across domestic differences that may exist amongst domestic privacy approaches*, https://www.apec.org/Groups/Committee- on- Trade- and- Investment/Electronic- Commerce- Steering- Group/, Ανάκτηση 17/2/2022

APEC, 2020 "*Member Economies*" , https://www.apec.org, Ανάκτηση 13/2/2022 About- Us/About- APEC/Member- Economies.aspx .

APEC , "*What is Asia-Pacific Economic Cooperation*?" at https://www.apec.org/About- Us/About- APEC/, Ανάκτηση 12/2/2022

Article 29 Data Protection Working Party. Advice paper on special categories of data ("sensitive data"). 2011 Apr 20. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf/, Ανάκτηση 1/2/2022

Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014 Apr. URL: https://ec.europa.eu/justice/article-29/press-material/public-consultation/notion-legitimate/, Ανάκτηση 1/2/2022

As-Saber S., Hossain K., Srivastava A. , 2007, *Technology, society and e-government: In search of an eclectic framework*. Electron. Gov. Int. J., 4, 156–178.

Asthmapolis, 2019, "*Asthmapolis, now propeller, moves beyond asthma*," http://tiny.cc/65gd5y/ Ανάκτηση 29/1/2022

B. Custers, F. Dechesne, A. M. Sears, T. Tani, and S. van der Hof, 2018, "A comparison of data protection legislation and policies across the eu*," Computer Law & Security Review*, vol. 34, no. 2, pp. 234–243.

Becky McCall,2018, *What does the GDPR mean for the medical community?* https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(18)30739-6/fulltext/ , Ανάκτηση 19/1/2022

Bekker H, 2018, *Gemeenten: Rijk moet tekorten sociaal domein bijpassen [Municipalities: state must match deficits social domain].* Binnenlands

Bestuur, 27 June. https://www.binnenlandsbestuur.nl/financien/nieuws/gemeenten-rijk-moet-tekorten-sociaal-domein.9591412.lynkx/, Ανάκτηση 3/2/2022

Beldad, A., De Jong, M., Steehouder, M. , 2011*, I trust not therefore it must be risky: Determinants of the perceived risks of disclosing personal data for e-government transactions*. Comput. Hum. Behav., 27, 2233–2242.

Bouman K., 2016*, Niet alles wat mogelijk is moet je willen.* [You shouldn't want everything that is possible]. *De Groene Amsterdammer,* 15 June, https://www.groene.nl/artikel/niet-alles-wat-mogelijk-is-moet-je-willen/, Ανάκτηση 26/1/2022

British Academy and Royal Society, 2017 *Data management and use: governance in the 21st century—a joint report by the British Academy and the Royal Society.*

Cabinet Office, 2016, Government Digital Service. *Data science ethical framework.*

Clare Sullivan, 2019*, EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era*, https://www.sciencedirect.com/science/article/abs/pii/S026736491930038X/, Ανάκτηση 1/2/2022

Cohen, J.E., 2012, *What privacy is for*. Harv. Law Rev. , 126, 1904.

Colin J. Bennett, 2018, *The European General Data Protection Regulation: An instrument for the globalization of privacy standards*? Ip, 23(2):239–246, Soon Ae Chun, Nabil R. Adam, and Beth Noveck, editors. ISSN: 15701255, 18758754. DOI: 1 0 . 3 2 3 3 / I P - 1 8 0 0 0 2 .

Colin Tankard, 2016, *What the GDPR means for businesses*, https://www.researchgate.net/publication/304607739_What_the_GDPR_means_for_businesses/, Ανάκτηση 29/1/2022

Contact Tracing Joint Statement. 2020 Mar 07. https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/, Ανάκτηση 3/2/2022

CoverUS,2019, "*Coverus, you shouldn?t have to be wealthy to be healthy.*" http://tiny.cc/cbhd5y/ Ανάκτηση 29/1/2022

Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer law & security review,* 34(1):134–153, 2018. ISSN: 0267-3649. DOI: 1 0 . 1 0 1 6 / j . c l s r . 2 0 1 7 . 0 5 . 0 1 5 .

Darcy W. E. Allen, Alastair Berg, Chris Berg, Brendan Markey-Towler, and Jason Potts. *Some Economic Consequences of the GDPR*. Economics Bulletin, 39(2):785–797, 2019. DOI: 1 0 . 2 1 3 9 / s s r n .

3 1 6 0 4 0 4 .

Daria Dubrova. *Challenges and Benefits of GDPR Implementation*. The App Solutions. 2018,

https://theappsolutions.com/blog/development/gdpr-challenges-and-benefits/, Ανάκτηση 18/1/2022

Data Protection Act 2018. legislation.gov.uk. 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/, Ανάκτηση 1/2/2022

Data Protection Act 2018 (Section 36(2)) (Health Research) *Regulations 2018*. 2018 Aug 10.

http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf/, Ανάκτηση 1/2/2022

'*Data Protection Regulation one year on: 73% of Europeans have heard of at least one of their rights'*. European Commission, 13 Jun 2019. http://europa.eu/rapid/press-release_IP-19-2956_en.htm/, Ανάκτηση 27/1/2022

'*Data Protection Regulation: one year on'*. European Commission, 22 May 2019. http://europa.eu/rapid/press-release_IP-19-2610_en.htm/ , Ανάκτηση 12/2/2022

D. D. Vergados, 2020, "Service personalization for assistive living in a

mobile ambient healthcare-networked environment," *Personal and*

Ubiquitous Computing, vol. 14, no. 6, pp. 575–590.

Diamantopoulou, V.; Androutsopoulou, A.; Gritzalis, S.; Charalabidis, Y., 2018, *An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance*. In Proceedings of the 2018 12th International Conference on Research Challenges in Information Science (RCIS), Nantes, France, 29–31 May 2018; pp. 1–9.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EUR-Lex. 1995 Nov 23. URL: https://eur-lex.europa.eu/eli/dir/1995/46/oj/, Ανάκτηση 2/2/2022

Dove ES. *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*. J Law Med Ethics 2019 Jan 10;46(4):1013-1030. [doi: 10.1177/1073110518822003]

ec.europa.eu, (2017), «*Ministerial Declaration on eGovernment – The Tallinn Declaration»*, https://ec.europa.eu/digital-

singlemarket/en/news/ministerial-declaration- egovernment-tallinn-declaration/ , Ανάκτηση 20/12/2021

EDPB. *European Data Protection Board (2019). First, Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities;* Technical Report; European Data Protection Board: Brussels, Belgium, 2019.

Edward S. Dove. *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*. J law med ethics, 46(4):1013–1030, 2018.ISSN: 1073-1105. DOI: 1 0 . 1 1 7 7 /1 0 7 3 1 1 0 5 1 8 8 2 2 0 0 3 .

Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis, 2018, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*. Journal of Cybersecurity, 4(1), ISSN:2057-2085, 2057-2093. DOI: 1 0 . 1 0 9 3 / c y b s e c /t y y 0 0 1.

E. R. Weitzman, L. Kaci, and K. D. Mandl, 2010, "*Sharing medical data for health research: the early personal health record experience,"* Journal of medical Internet research*,* vol. 12, no. 2.

Erik van der Marel, Matthias Bauer, Hosuk LeeMakiyama, and Bert Verschelde. *A methodology to estimate the costs of data regulations.* International Economics, (146):12–39, 2016. DOI: 1 0 . 1 0 1 6 / j .i n t e c o . 2 0 1 5 . 1 1 . 0 0 1 .

EU. *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation);* Publications Office of the European Union: Luxembourg, 2016.

European Commission A Privacy Impact Assessment Framework for Data Protection and Privacy Rights; Technical Report ISO: Cham, Switzerland, 2012.

European Data Protection Board. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of* the COVID-19 outbreak. 2020 Apr 21. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf/ , Ανάκτηση 1/2/2022

European Data Protection Board. *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR*) (art. 70.1.b)). 2019 Jan 23. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf/, Ανάκτηση 30/1/2022

European Data Protection Board. *Guidelines 02/2018 on derogations of Article 49 under Regulation 2016/679. 2018 May 05.* https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf/, Ανάκτηση 4/2/2022

European Data Protection Board. *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*. 2020 Apr 21. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200_3_healthdatascientificresearchcovid19_en.pdf/, Ανάκτηση 31/1/2022

European Data Protection Board. *EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*. 2020 Mar 19.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf/, Ανάκτηση 2/2/2022

European Data Protection Board. *Guidelines 05/2020 on consent under Regulation 2016/679* (Version 1.1). 2020 May 04, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf/, Ανάκτηση31/1/2022

European Data Protection Board. *Statement on the processing of personal data in the context of the COVID-19 outbreak*. 2020 Mar 19, https://edpb.europa.eu/sites/edpb/files/files/file1/, Ανάκτηση 4/2/2022

European Data Protection Supervisor. *A Preliminary Opinion on data protection and scientific research*. 2020 Jan. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf/ , Ανάκτηση 31/1/2022

European Union (Withdrawal) *Act 2018*. legislation.gov.uk. 2018 Jun 28.https://www.legislation.gov.uk/ukpga/, Ανάκτηση 30/1/2022

Facebook: *Υποκλαπέντα δεδομένα 87 εκατ. Χρηστών*, 2018

http://www.kathimerini.gr/957812/article/epikairothta/kosmos/facebook-ypoklapenta-dedomena-87-ekat-xrhstwn/, Ανάκτηση 26/1/2022

F. D. Davis and P. R. Warshaw, 1992, "What do intention scales measure?" *The Journal of General Psychology*, vol. 119, no. 4, pp. 391–407.

First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities'. European Data Protection Board, 2019.
https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_lib/ , Ανάκτηση 28/1/2022

Floridi L, Taddeo M. 2016 *What is data ethics?* Phil. Trans. R. Soc. A 374, 20160360. (doi:10.1098/rsta.2016.0360)

"*Flue Near You*, 2019, http://tiny.cc/sihd5y/ , Ανάκτηση 17/1/2022

Fuzzy Logix,2019, "*Opioid abuse prediction-fuzzy logix*," http://tiny.cc/o7gd5y/, Ανάκτηση 29/1/2022

Gary Miglicco, 2018, *GDPR is here and it is time to get serious*. Computer fraud & security, 2018(9):9–12, 2018. ISSN: 1361-3723. DOI: 1 0 . 1 0 1 6 / S 1 3 6 1 - 3 7 2 3 (1 8) 3 0 0 8 5 - X .

Georgieva L, Docksey C. *Processing of special categories of personal data*. In: Kuner C, Bygrave LA, Docksey C, editors. The EU General Data Protection Regulation (GDPR): A Commentary. New York, NY: Oxford University Press; 2020:365-384, doi: 10.1093/oso/9780198826491.001.0001, ISBN: 9780198826491.

Gerard Buckley, Tristan Caulfield & Ingolf Becker, 2021, "*It may be a pain in the backside but...Insights into the impact of GDPR on business after three years*." University College London, https://arxiv.org/abs/2110.11905/ , Ανάκτηση 2/2/2022

General Data Protection Regulation'. Wikipedia. 2016. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation/ , Ανάκτηση 10/2/2022

Gonçalo Almeida Teixeira, Miguel Mira da Silva and Ruben Pereira. The critical success factors of GDPR implementation: *A systematic literature review. Digital Policy, Regulation and Governance*, 21(4):402–418, 2019. ISSN: 2398-5038. DOI: 1 0 . 1 1 0 8 / D P R G - 0 1 - 2 0 1 9 - 0 0 0 7 .

Guide to the General Data Protection Regulation (GDPR). *Information Commissioner's Office (ICO*). 2020 Apr 25. https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulation-gdpr/, Ανάκτηση 30/1/2022

Hallinan D., 2020, *Broad consent under the GDPR: an optimistic perspective on a bright future.* Life Sci Soc Policy 2020 Jan 06;16(1):1 [FREE Full text] [doi: 10.1186/s40504-019-0096-3] [Medline: 31903508]

Hartholt S., 2017, Data brengen de burger in beeld [Data makes the citizen visible]. *Binnenlands Bestuur*, 23 June.

https://www.binnenlandsbestuur.nl/digitaal/achtergrond/achtergrond/data-brengen-de-burger-in-beeld.9572969.lynkx/, Ανάκτηση 19/1/2022

"*Healthmap*", 2019, http://tiny.cc/0jhd5y/ Ανάκτηση 30/1/2022

He Li, Lu Yu, and Wu He. *The Impact of GDPR on Global Technology Development. Journal of global information technology management*, 22(1):1–6, 2019. ISSN: 1097-198X, 2333-6846. DOI: 1 0 . 1 0 8 0 /1 0 9 7 1 9 8 X . 2 0 1 9 . 1 5 6 9 1 8 6 .

Henderson, S.E., 2012, *Expectations of privacy in social media*. Miss CL Rev., 31, 227.

IAAP, 2018, *Privacy Tech Vendor Report*; Technical Report; IAPP: Portsmouth, NH, USA.

I. Ajzen, 1991, "The theory of planned behavior," *Organizational behavior and human decision processes*, vol. 50, no. 2, pp. 179–211.

IBM Big data and analytics Hub,2019, "*Big data in healthcare: Tapping new insight to save lives*," http://tiny.cc/43gd5y/, Ανάκτηση 30/1/2022

IBP , 2018, *Rijk, Gemeenten, Provincies en Waterschappen Starten met een Interbestuurlijk Programma en een Gezamenlijke Agenda*. [Kingdom, municipalities, provinces and water councils form a joint agenda]. https://vng.nl/files/vng/brieven/2018/attachments/programmastart_ibp.pdf/ ,Ανάκτηση 3/2/2022

ICO, 2007, *Privacy Impact Assessment Handbook, Wilmslow, Cheshire, UK, Version 1.0*; Trilateral Research and Consulting, Technical Report; ICO: Wilmslow, UK.

Isabel Maria Lopes and Pedro Oliveira, 2018*, Implementation of the general data protection regulation: A survey in health clinics*. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI).13th Iberian Conference on Information Systems and Technologies (CISTI), pages 1–6, 2018. DOI: 1 0 . 2 3 9 1 9 / C I S T I . 2 0 1 8 . 8 3 9 9 1 5 6 .

ISACA, 2018, *GDPR: The end of the Beginning;* Technical Report; ISACA: Rolling Meadows, IL, USA.

Islam, M.B., Watson, J., Iannella, R., Geva, S., 2014, *What I Want for My Social Network Privacy;* NICTA: Sydney, Australia.

ISO/IEC. ISO FDIS 29134, 2017, *Information Technology–Security Techniques–Privacy Impact Assessment–Guidelines; Technical Report ISO: Cham*, Switzerland.

Jan Philipp Albrecht, 2016, *How the GDPR Will Change the World,* http://edpl.lexxion.eu/ , Ανάκτηση 14/2/2022

Javid Khan. The need for continuous compliance. *Network security*, 2018(6):14–15, 2018. ISSN: 1353-4858. DOI: 1 0 . 1 0 1 6 / S 1 3 5 3 - 4 8 5 8 (1 8) 3 0 0 5 7 - 6 .

J. Kaye, L. Curren, N. Anderson, K. Edwards, S. M. Fullerton, N. Kanellopoulou, D. Lund, D. G. MacArthur, D. Mascalzoni, J. Shep-

herd et al., 2012, “From patients to partners: participant-centric initiatives in biomedical research,” *Nature Reviews Genetics*, vol. 13, no. 5, p. 371.

J. Koster, E. Stewart, and E. Kolker, 2016, "*Health care transformation: A strategy rooted in data and analytics*," Academic Medicine, vol. 91, no. 2, pp. 165–167.

Joanna Kessler. *Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource" Notes*. S. cal. l. rev., 93(1):99–128, 2019–2020.

Joe Garber, 2018, *GDPR – compliance nightmare or business opportunity? Computer fraud & security*, 2018(6):14–15, 2018. ISSN: 1361-3723. DOI: 1 0 . 1 0 1 6 / S 1 3 6 1 - 3 7 2 3 (1 8) 3 0 0 5 5 - 1 .

Kitchin R, Lauriault TP and McArdle G, 2015, *Knowing and governing cities through urban indicators, city benchmarking and real-time dashboards.* Regional Studies, Regional Science 2(1), 6–28.

Kitchin R, Maalsen S and McArdle G, 2016, *The praxis and politics of building urban dashboards*. Geoforum 77, 93–101.

K. K. Kim, P. Sankar, M. D. Wilson, and S. C. Haynes,2017, "Factors

affecting willingness to share electronic health data among California consumers," *BMC medical ethics*, vol. 18, no. 1, p. 25.

Kriens J , 2016 Commentaar: Sturen met Data [Comment: Data steering]. *Vereniging Nederlandse Gemeenten*. https://vng.nl/producten-diensten/vng-magazine/vng-magazine-nummer-9-2016/sturen-met-data/ , Ανάκτηση 26/1/2022

Kuner C, Bygrave L, Docksey C, 2020, *Background and Evolution of the EU General Data Protection Regulation*. In: Kuner C, Bygrave LA, Docksey C, editors. The EU General Data Protection Regulation (GDPR): A Commentary. New York, NY: Oxford University Press; 2020:1-47.

Lag (2003:460) om *etikprövning av forskning som avser människor.* Webpage in Swedish. Regeringskansliet. 2003 Jun 05, http://rkrattsbaser.gov.se/sfst?bet=2003:460/, Ανάκτηση 1/2/2022

Lash, S., Szerszynski, B., Wynne, B., 1996, *Risk, Environment and Modernity: Towards a New Ecology*, Sage: Newcastle upon Tyne, UK, Volume 40.

Liesbet van Zoonen, 2020*, Data governance and citizen participation in the digital welfare state,* https://www.cambridge.org/core/journals/data-and-policy/article/data-governance-and-citizen-participation-in-the-digital-welfare-state/CCF2E1914C7E2D4593D550C6BC9E4C70/, Ανάκτηση 26/1/2022

Lov om behandling av personopplysninger (personopplysningsloven). Wepage in Norwegian. Lovdata. 2018 Jul 20, https://lovdata.no/dokument/NL/lov/2018-06-15-38/, Ανάκτηση 1/2/2022

Luciano Floridi, 2018, *Soft ethics, the governance of the digital and the General Data Protection Regulation*. Phil. Trans. R. Soc. A 376Q20180081, http://dx.doi.org/10.1098/rsta.2018.0081/, Ανάκτηση 4/2/2022

Maria Addis and Maria Kutar, 2018, The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. *UK Academy for Information Systems Conference Proceedings* 2018.

Marx, G.T., 2001, Murky conceptual waters: *The public and the private*. *Ethics Inf. Technol*. , 3, 157–169.

Medaglia, R., 2006–2011 e-Participation research: *Moving characterization forward* (2006–2011). Gov. Inf. Q. 2012, 29, 346–360.

Mergel I., Kattel R., Lember V., Mcbride K., 2018, «*Citizen – Oriented Digital Transformation in the Public Sector*», 19th Annual International Conference, May

M. Fishbein and I. Ajzen, 1975, *Belief, attitude, intention and behavior: An introduction to theory and research*.

Miinome,2019, "*Miinome - it's in your dna*," http://tiny.cc/4dhd5y/ Ανάκτηση 29/1/2022

Mitrou, L*., 2002, Law in the Information Society*, Sakkoulas Publications: Athens, Greek.

Mitrou, L. *General Data Protection Regulation: New Law–New Obligations–New Rights*, Sakkoulas Publications: Athens, Greek, 2017.

M. Karampela, S. Ouhbi and M. Isomursu, 2019, *Exploring users' willingness to share their health and personal data under the prism of the new GDPR: implications in healthcare,* https://ieeexplore.ieee.org/document/8856550/, Ανάκτηση 15/2/2022

Mohamed, N.; Ahmad, I.H. *Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia.* Comput. Hum. Behav. 2012, 28, 2366–2375.

Nazar Poritskiy, Flávio Oliveira, and Fernando Almeida, 2019, *The benefits and challenges of general data protection regulation for the information technology sector. Digital Policy, Regulation and Governance,* 21(5):510–524, 2019. ISSN: 2398-5038. DOI: 1 0. 1 1 0 8 / D P R G - 0 5 - 2 0 1 9 - 0 0 3 9 .

Newburn, T., Jones, T. *Private Security and Public Policing*, Clarendon Press: Oxford, UK, 1998.

Nick Wallace and Daniel Castro, 2018, *The Impact of the EU's New Data Protection Regulation on AI, Centre for Data Innovation*.

Noord-Hollands Dagblad , 2015. *Wijken Verkennen via de Computer.* [Exploring Neighborhoods by Computer].

https://www.bigdata.company/artikel-huiselijk-geweld-monitor/, Ανάκτηση 26/1/2022

Oxford Analytica. *Europe's national regulators hold key to GDPR success.* Emerald Expert Briefings, oxan db, oxan-db, 2019. ISSN: 2633-304X. DOI: 1 0 . 1 1 0 8 / O X A N - D B 2 4 3 9 1 6 .

Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, and Ignacio Sanchez. *The right to data portability in the GDPR: Towards user- centric interoperability of digital services. Computer law & security review*, 34(2):193–203, 2018. ISSN:

0267-3649. DOI: 1 0 . 1 0 1 6 / j . c l s r . 2 0 1 7 . 1 0 . 0 0 3 .

Peloquin D, DiMaio M, Bierer B, Barnes M. Disruptive and avoidable: *GDPR challenges to secondary research uses of data*. Eur J Hum Genet 2020 Jun;28(6):697-705. [doi: 10.1038/s41431-020-0596-x] [Medline: 32123329]

Personuppgiftsbehandling för forskningsändamål SOU 2017. Webpage in Swedish. Regeringskansliet. 2019 Jun 09. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2017/06/sou-201750/ Ανάκτηση 2/2/2022

Peter Lindgren. *GDPR Regulation Impact on Different Business Models and Businesses*. Journal of Multi Business Model Innovation and Technology, 4(3):241–254, 2016. ISSN: 2245-456X, 2245-8832. DOI: 1 0. 1 3 0 5 2 / j m b m i t 2 2 4 5 - 4 5 6 X . 4 3 4 .

Phil Beckett, 2017, *GDPR compliance: Your tech department's next big opportunity*. Computer fraud & security, 2017(5):9–13, ISSN: 1361-3723. DOI: 1 0 . 1 0 1 6 / S 1 3 6 1 - 3 7 2 3 (1 7) 3 0 0 4 1 - 6

Pierucci A, Walter JP. Joint Statement on the right to data protection in the context of the COVID-19 pandemic. Council of Europe. 2020 Mar 30. URL: https://www.coe.int/en/web/data protection/, Ανάκτηση 30/1/2022

Police (2017) *Criminaliteits Anticipatie Systeem verder uitgerold bij Nationale Politie*. [Further roll out of Criminality Anticipation

System]. https://www.politie.nl/nieuws/2017/mei/15/05-cas.html/, Ανάκτηση 5/2/2022

P. Samarati and S. D. C. Di Vimercati, 2010, "Data protection in outsourcing scenarios: Issues and directions*," in Proceedings of the 5th ACM Symposium on Information*, *Computer and Communications Security.* ACM, pp. 1–14.

Raccolta delle principali disposizioni adottate in relazione allo stato di emergenza epidemiologica da Covid-19 aventi implicazioni in materia di protezione dei dati personali. *Garante per la protezione dei dati personali*. 2020 Jun 25. https://tinyurl.com/y7499zyg/, Ανάκτηση 4/2/2022

Radar (2017) *Bijstandsuitkering Kwijt Door Pinpas van Demente Moeder.* [Cut from Benefits Because of Mother's Bank Card].

https://radar.avrotros.nl/uitzendingen/gemist/item/bijstandsuitkering-kwijt-door-pinpas-van-demente-moeder/, Ανάκτηση 26/1/2022

Ralph O'Brien, 2016, *Privacy and security: The new European data protection regulation and it's data breach notification requirements*. Business information review, 33(2):81–84, ISSN: 0266-3821. DOI: 1 0 . 1 1 7 7 / 0 2 6 6 3 8 2 1 1 6 6 5 0 2 9 7 .

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and

repealing Directive 95/46/EC (General Data Protection Regulation), OJEU L119, 04/05/2016.

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Publications Office of the European Union. 2016 Apr 27. URL:https://op.europa.eu/,Ανάκτηση 30/1/2022

'*Regulation (EU) 2016/679 of the European Parliament and of the Council*'. Europa, 2016. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf/, Ανάκτηση 11/2/2022

Rubio AI, 2018, *Aanvragen bijstand bij gemeente expres lastig* [Very difficult to request benefits from the municipality]. Algemeen Dagblad, 11 April,

https://www.ad.nl/rotterdam/aanvragen-bijstand-bij-gemeente-expres-lastig~a62e30aa/, Ανάκτηση 26/1/2022

Sarah Shyy, 2020, *The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business*. U.c. davis bus. l.j., 20(2):137–164.

Sharing research data and findings relevant to the novel coronavirus (COVID-19) outbreak. Wellcome. URL: https://wellcome.ac.uk/coronavirus-covid-19/open-data/, Ανάκτηση 30/1/2022

Solove, D.J. *A taxonomy of privacy*. Univ. Pa. Law Rev. 2005, 154, 477

Spiekermann, S.; Acquisti, A.; Böhme, R.; Hui, K.L. *The challenges of personal data markets and privacy.* Electron. Mark. 2015, 25, 161–167.

Stanford Medice, 2019, "*Big data = big finds: Clinical trial for deadly*

lung cancer launched by stanford study," http://tiny.cc/j9gd5y/, Ανάκτηση 29/1/2022

S. Taylor and P. A. Todd, 1995, "*Understanding information technology usage: A test of competing models*," Information systems research, vol. 6, no. 2, pp. 144–176.

Steiner B., 2018,a*, Ruimte en Risico's. Een Verkenning van de Financiele Gevolgen van het Interbestuurlijk Programma voor het Sociaal Domein* [Options and risks: an exploration of the financial consequences of the inter-administrative programme for the social domain]. Utrecht, The Netherlands: Divosa. https://www.divosa.nl/sites/default/files/onderwerp_bestanden/rapport-ibp-en-financien-sociaal-domein.pdf/, Ανάκτηση 26/1/2022

Steiner B., 2018, b, *Sociaal Domein Kostte in 2017 4,4% Meer dan Begroot* [Social domain costs 4,4% higher than expected]. Utrecht, The Netherlands: Divosa, https://www.binnenlandsbestuur.nl/Uploads/2018/10/divosa-rapport-gemeente lijke-financien-sociaal-domein-rekening-2017.pdf/, Ανάκτηση 26/1/2022

Stephane Ciriani, 2015, *The Economic Impact of the European Reform of Data Protection. Communications & Strategies*, 97:41–58, 1st quarter 2015.

Stimulansz (n.d.), 2019, *Big Data in het Sociaa Domein* [Big Data in the Social Domain], https://www.stimulansz.nl/advies/big-data/, Ανάκτηση 26/1/2022

Susha, I., Grönlund, &. eParticipation research: *Systematizing the field.* Gov. Inf. Q. 2012, 29, 373–382.

S. Wachter, 2018, "*Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr*," Computer law & security review, vol. 34, no. 3, pp. 436–449.

The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers. European Law Blog. 2020 Apr 03. https://europeanlawblog.eu/2020/04/03/the-coronavirus-crisis-and-eu-adequacy-decisions-for-data-transfers/, Ανάκτηση 1/2/2022

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, legislation.gov.uk. 2019, https://www.legislation.gov.uk/uksi/2019/419/contents/made/, Ανάκτηση 31/1/2022

Thomson Reuters, 2019. *Study Finds Organizations Are Not Ready for GDPR Compliance Issues*; Technical Report; 2019. https://legal.thomsonreuters.com/en/insights/articles/study-finds-organizations- not-ready-gdpr-compliance-issues/, Ανάκτηση 6/2/2022

T. Hub, 2019, "*The Hub of all things*," http://tiny.cc/vchd5y/, Ανάκτηση 29/1/2022

Tietosuojalaki 1050/2018. Webpage in Finnish. Finlex. 2018 Dec 04., https://www.finlex.fi/fi/laki/alkup/2018/20181050/, Ανάκτηση 31/1/2022

Uitvoeringswet Algemene verordening gegevensbescherming. Webpage in Dutch. Overheid.nl. 2019 Feb 19. https://wetten.overheid.nl/BWBR0040940/2019-02-19/, Ανάκτηση 3/2/2022

Virkar S., Edelmann N., Hynek N., Parycek P., (2019), «*Digital Transformation in Public Sector Organizations: the role of informal knowledge sharing networks and social media*», Electronic Participation, July

V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, 2003, *"User acceptance of information technology: Toward a unified view*," *MIS quarterly*, pp. 425–478.

VNG/Berenschot (2018) *Datagedreven Sturing Bij Gemeenten*. https://vng.nl/files/vng/nieuws_attachments/2018/datagedreven_sturing_bij_gemeenten_lr.pdf/ ,Ανάκτηση 5/2/2022

Y. Wang, L. Kung, W. Y. C. Wang, and C. G. Cegielski, "*An integrated*

big data analytics-enabled transformation model: Application to health care," Information & Management, vol. 55, no. 1, pp. 64–79, 2018.

Wang Kaushik. *Data Privacy: Demystifying The GDPR. iSchool | Syracuse University, 2018*, https://ischool-dev.syr.edu/data-privacy -demystifying -gdpr/ , Ανάκτηση 17/1/2022

Wiewiórowski W. EU Digital Solidarity: *a call for a pan-European approach against the pandemic. European Data Protection Supervisor.* 2020 Apr 06. https://edps.europa.eu/sites/edp/files/publication/, Ανάκτηση 2/2/2022

2020-04-06_*eu_digital_solidarity_covid19_en.pdf*

Wright, D., De Hert, P. *Introduction to privacy impact assessment. In Privacy Impact Assessment;* Springer: Dordrecht, The Netherlands, 2012; pp. 3–32.

Working Party 29. *Guidelines on Data Protection Impact Assessment*; Technical Report ISO: Cham, Switzerland, 2019.

World Health Organization, 2016, "*Global Diffusion of eHealth: Making Universal Health Coverage Achievable: Report of the Third Global Survey on e-Health,*" https://goo.gl/Fd3VwP/, Ανάκτηση 27/1/2022

W. Raghupathi and V. Raghupathi, "*Big data analytics in healthcare:*

promise and potential," Health information science and systems, vol. 2, no. 1, p. 3, 2014