ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΠΛΗΡΟΦΟΡΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΟΙΚΟΝΟΜΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Διδακτορική Διατριβή

Σταυρούλα Φ. Ρίζου

Τριμελής Επιτροπή

Καθηγήτρια Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου (Επιβλέπουσα)

Αν. Καθηγητής Κωνσταντίνος Ψάννης (Μέλος)

Αν. Καθηγητής Κωνσταντίνος Φούσκας (Μέλος)

Η παρούσα διδακτορική διατριβή υποστηρίχθηκε από το
Ελληνικό Ίδρυμα Έρευνας και Καινοτομίας (ΕΛΙ.Δ.Ε.Κ.) στο πλαίσιο της Δράσης
«Υποτροφίες ΕΛΙ.Δ.Ε.Κ. Υποψηφίων Διδακτόρων» (Αριθμός Υποτροφίας: 290)

ΕΥΧΑΡΙΣΤΙΕΣ

Εν πρώτοις, θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα Καθηγήτρια του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας, κ. Ευγενία Αλεξανδροπούλου–Αιγυπτιάδου, για την ανάθεση της διατριβής αυτής, για την καθοδήγησή της στη συγγραφή της παρούσας διατριβής καθώς και τις ιδιαίτερα πολύτιμες συμβουλές της.

Επίσης, ευχαριστώ πολύ τα μέλη της Τριμελούς Επιτροπής, τον Αν. Καθηγητή του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας, κ. Κωνσταντίνο Ψάννη και τον Αν. Καθηγητή του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας, κ. Κωνσταντίνο Φούσκα. Εκτός αυτού, θα ήθελα να ευχαριστήσω τον Αν. Καθηγητή, κ. Κωνσταντίνο Ψάννη για την υποστήριξη και την πολύτιμη βοήθεια που μου παρείχε στην εκπόνηση του ερευνητικού μου έργου και στη διάχυση αυτού. Παράλληλα, θα ήθελα να ευχαριστήσω όλα τα μέλη της Επταμελούς Εξεταστικής Επιτροπής, τον Καθηγητή του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας, κ. Εμμανουήλ Στειακάκη, τον Καθηγητή του Τμήματος Νομικής του Δημοκρίτειου Πανεπιστημίου Θράκης, κ. Χρήστο Μαστροκώστα, την Αν. Καθηγήτρια του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Μακεδονίας, κ. Δέσποινα Αναγνωστοπούλου, και τον Επίκουρο Καθηγητή του Τμήματος Ανθρωπιστικών, Κοινωνικών και Οικονομικών Επιστημών του Διεθνούς Πανεπιστημίου Ελλάδος, κ. Κομνηνό Κόμνιο.

Θα ήθελα να ευχαριστήσω το Ελληνικό Ίδρυμα Έρευνας και Καινοτομίας (ΕΛΙ.Δ.Ε.Κ.) για την οικονομική υποστήριξη της παρούσας διατριβής.

Τέλος, ευχαριστώ την οικογένειά μου για τη στήριξή τους σε όλα τα στάδια των σπουδών μου.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

I. ΕΛΛΗΝΟΓΛΩΣΣΕΣ

ΕΕ	Ευρωπαϊκή Ένωση
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΠΟΕ	Παγκόσμιος Οργανισμός Εμπορίου
ΕΟΧ	Ευρωπαϊκός Οικονομικός χώρος

II. ΞΕΝΟΓΛΩΣΣΕΣ

4G	Fourth generation (Ασύρματα δίκτυα $4^{ης}$ γενιάς)
5G	Fifth generation (Ασύρματα δίκτυα $5^{ης}$ γενιάς)
6G	Sixth generation (Ασύρματα δίκτυα 6ης γενιάς)
AI	Artificial Intelligence (Τεχνητή νοημοσύνη)
GDPR	General Data Protection Regulation
IP	Internet protocol (Πρωτόκολλο του Διαδικτύου)
MIMO	multiple-input and multiple-output
PIA	Privacy Impact Assessment
IoT	Internet of things (Διαδίκτυο των Πραγμάτων)
GATS	General Agreement on Trade in Services
PNR	Passenger name records (Καταστάσεις ονομάτων επιβατών)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TFTP	Terrorist Finance Tracking Program (Πρόγραμμα Ανίχνευσης της Χρηματοδότησης της Τρομοκρατίας)

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΓΡΑΦΗΜΑΤΩΝ

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας διδακτορικής διατριβής είναι η μελέτη, ανάλυση και καταγραφή της νομικής προσέγγισης του πλαισίου της διασυνοριακής ροής των οικονομικών δεδομένων. Η διακίνηση των προσωπικών οικονομικών δεδομένων, ως φαινόμενο της σύγχρονης τεχνολογικής και οικονομικής πραγματικότητας αναδύει ζητήματα των οποίων η διερεύνηση απαιτεί τη σύμπλευση αφενός της Επιστήμης της Πληροφορικής και αφετέρου της Νομικής Επιστήμης. Το παρόν πόνημα εστιάζει στην ταχεία εξέλιξη των νομοθετημάτων που αφορούν την προστασία των προσωπικών δεδομένων και ειδικότερα το πεδίο της διασυνοριακής ροής των δεδομένων.

Εν πρώτοις, οι στόχοι της παρούσας διατριβής πραγματώνονται με την ανάλυση της έννοιας και των προσεγγίσεων της διασυνοριακής ροής των προσωπικών δεδομένων καθώς και των διακρίσεων των οικονομικών δεδομένων. Επιπλέον, εξετάζεται το γενικό ρυθμιστικό πλαίσιο των οικονομικών δεδομένων με γνώμονα τα ζητήματα ιδιωτικότητας, συμπεριλαμβανομένου του περιβάλλοντος της διασυνοριακής ροής των φορολογικών δεδομένων, των χρηματοοικονομικών δεδομένων και της διασυνοριακής ροής των δεδομένων στο διεθνές εμπόριο. Το οντολογικό μέρος της διατριβής συμπληρώνεται από τη συσχέτιση των ζητημάτων ιδιωτικότητας με επιλεγμένες σύγχρονες τεχνολογίες του τομέα της Πληροφορικής, και ειδικότερα τα δίκτυα 5G, τα αναδυόμενα δίκτυα 6G και την αλληλεπίδραση των ανηλίκων με ένα έξυπνο οικιακό περιβάλλον.

Παράλληλα, στο παρόν πόνημα περιλαμβάνεται η συστηματική και διαχρονική ανάλυση των διεθνών, ευρωπαϊκών και εθνικών ρυθμίσεων, οι οποίες διέπουν το εξειδικευμένο πεδίο της διασυνοριακής ροής των προσωπικών δεδομένων, με επίκεντρο τη διαφορετική νομική προσέγγιση για την προστασία των οικονομικών προσωπικών δεδομένων από τα κράτη καθώς και τις προσπάθειες γεφύρωσης αυτών.

Λέξεις κλειδιά: διασυνοριακή ροή δεδομένων, οικονομικά δεδομένα, προσωπικά δεδομένα, GDPR, ιδιωτικότητα, ασφάλεια

ABSTRACT

The object of this doctoral dissertation is the research, analysis and description of the legal approach regarding the framework of the cross-border flows of economic data. The transmission of personal economic data, as a phenomenon of modern technological and economic reality, raises issues whose investigation requires the conflation of both Computer Science and Legal Science. This study focuses on the rapid evolution of legislation concerning the protection of personal data and in particular the field of cross-border data flows.

First of all, the objectives of this thesis are realized by analyzing the concept and approaches of the cross-border flows of personal data as well as the distinctions of economic data. In addition, the general regulatory framework of economic data is examined in the light of privacy issues, including the environment of the cross-border flows of tax data, financial data and the cross-border data flows in international trade. The ontological part of the thesis is complemented by the correlation of privacy issues with selected modern technologies in the IT sector, in particular 5G networks, emerging 6G networks and the interaction of minors with a smart home environment.

In parallel, this study includes the systematic and intertemporal analysis of international, European and national regulations, which govern the specialized field of the cross-border flows of personal data, focusing on the different legal approaches to the protection of economic personal data, at State level, as well as the efforts to bridge them.

Key words: cross-border data flows, economic data, personal data, GDPR, privacy, security

ΕΙΣΑΓΩΓΗ

Η σύγχρονη εξελισσόμενη αναβάθμιση του παγκόσμιου ιστού και οι καινοτομίες των τεχνολογιών πληροφοριών και επικοινωνιών, εν γένει, έχουν αναντίρρητη επιρροή στο δίκαιο των προσωπικών δεδομένων σε παγκόσμιο επίπεδο, ως απόρροια της αλλεπάλληλης γένεσης νέων παραγόντων που επηρεάζουν το υφιστάμενο καθεστώς. Αυτό το γεγονός οφείλεται στον ρόλο των προσωπικών δεδομένων στο σύγχρονο κοινωνικό και οικονομικό πλαίσιο, ο οποίος έχει αναχθεί σε παράγοντα καίριας σημασίας[1].

Από τη δεκαετία του 1970, σε παγκόσμιο επίπεδο, η υιοθέτηση νομοθεσιών για την προστασία των προσωπικών δεδομένων εμφανίζει συνεχόμενη αύξηση, κυρίως μετά τη δεκαετία του 2000[2]. Εν γένει, οι ραγδαίες νομοθετικές εξελίξεις έχουν μεταβάλει το πεδίο της προστασίας των προσωπικών δεδομένων, εγείροντας ανοιχτά επιστημονικά ζητήματα ως προς τον αντίκτυπο που θα επιφέρει το υφιστάμενο καθεστώς. Η απαραίτητη διασυνοριακή συνεργασία, η οποία αποτελεί αναπόσπαστο παράγοντα της οικονομικής ανάπτυξης, με τη συνεχή εξέλιξη της τεχνολογίας, έχει αναδείξει την ανάγκη εστίασης στη διασυνοριακή έκφανση της προστασίας των προσωπικών δεδομένων. Στο επίκεντρο της παρούσας διατριβής βρίσκεται η αποσαφήνιση, κυρίως των οικονομικών δεδομένων σε διασυνοριακό επίπεδο, λόγω της σπουδαίας αλληλεπίδρασης του περιβάλλοντός τους με τις τεχνολογίες πληροφοριών και επικοινωνιών. Πιο συγκεκριμένα, θα πρέπει να σημειωθεί ότι ο χρηματοοικονομικός τομέας συγκεντρώνει όγκο δεδομένων[3], ο οποίος αποτελεί ένα από τα μεγαλύτερα μεγέθη μεταξύ των άλλων τομέων δραστηριοτήτων.

Όπως έχει υποστηριχθεί[4], η νομοθεσία που διέπει την προστασία των διασυνοριακών ροών των δεδομένων θα πρέπει να εστιάζει, όχι μόνο σε θεσμικά και διαχειριστικά σημεία, αλλά και στην προστασία των μεταφερόμενων δεδομένων ήδη από τον σχεδιασμό, λαμβάνοντας υπόψη τις εκάστοτε τεχνολογικές εξελίξεις. Συλλήβδην, η διακίνηση των προσωπικών οικονομικών δεδομένων εγείρει ζητήματα τα οποία εδράζονται στα επιστημονικά πεδία τόσο της Νομικής Επιστήμης όσο και της Επιστήμης της Πληροφορικής. Η παρούσα μελέτη ενισχύει, προς την κατεύθυνση αυτή, την ακαδημαϊκή κατανόηση των παραγόντων οι οποίοι θα πρέπει να ληφθούν υπόψη κατά το σχεδιασμό και την εφαρμογή των τεχνολογιών, υπό νομικό πρίσμα. Η πολυπαραγοντική ανάλυση

[1] Casalini, F., & González, J. L. (2019). Trade and cross-border data flows.

[2] Casalini, F., & González, J. L. (2019). Trade and cross-border data flows.

[3] OECD. (2015). *Data-driven innovation: Big data for growth and well-being*.

[4] Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p.175.

της νομικής προσέγγισης των διασυνοριακών ροών των δεδομένων στην παρούσα διατριβή, με σημείο αναφοράς την ευρωπαϊκή νομοθεσία, στοχεύει στη βέλτιστη αποσαφήνιση του πλαισίου τους. Παράλληλα, κύριο στόχο συνιστά η διατύπωση προτάσεων de lege ferenda για ένα αποτελεσματικό θεσμικό πλαίσιο, το οποίο να περιβάλλει τη διασυνοριακή ροή των οικονομικών προσωπικών δεδομένων.

Ειδικότερα, θα πρέπει να σημειωθεί ότι η ενωσιακή νομοθεσία για την προστασία των προσωπικών δεδομένων έχει μετασχηματίσει το τοπίο της προστασίας της ιδιωτικότητας, όχι μόνο σε ευρωπαϊκό επίπεδο με την άμεση εφαρμογή του Γενικού Κανονισμού για την Προστασία Δεδομένων (General Data Protection Regulation, GDPR) τον Μάιο 2018 στα κράτη-μέλη αλλά και σε παγκόσμιο επίπεδο με την προβλεπόμενη διευρυμένη εμβέλειά του. Ως εκ τούτου, στην παρούσα μελέτη επιχειρείται η διερεύνηση του αντίκτυπου αυτού του σύγχρονου νομικού εργαλείου για την προστασία των προσωπικών δεδομένων.

Η παρούσα διατριβή οδηγεί σε μια διαδικασία ανάδειξης του πλαισίου της διασυνοριακής ροής των οικονομικών δεδομένων με τη μέθοδο της βιβλιογραφικής ανασκόπησης, αποτελούμενη από δύο μέρη. Το πρώτο μέρος περιλαμβάνει την οντολογική θεώρηση του πεδίου, επιδιώκοντας την ανάδειξη των καίριων και σύγχρονων παραγόντων καθορισμού του. Το δεύτερο μέρος εξετάζει τις νομικές ρυθμίσεις του πεδίου σε επίπεδο διεθνών, εθνικών και ευρωπαϊκών νομοθεσιών εστιάζοντας στη διαφορετική νομική προσέγγιση της προστασίας των οικονομικών προσωπικών δεδομένων καθώς και στη διαδικασία σύμπλευσης αυτών. Παράλληλα, θα πρέπει να αναφερθεί ότι στο παρόν πόνημα εντάσσονται τέσσερις δημοσιευμένες ερευνητικές εργασίες.

Με βάση τα προαναφερθέντα, η διάρθρωση της παρούσας διατριβής αποτελείται από δέκα αυτοτελή κεφάλαια.

Πιο συγκεκριμένα, στο πρώτο κεφάλαιο, παρουσιάζεται ο εννοιολογικός προσδιορισμός του όρου της διασυνοριακής ροής των δεδομένων καθώς και οι προσεγγίσεις της έννοιας, προκειμένου αφενός να οριοθετηθεί το πεδίο και αφετέρου να διατυπωθούν οι θεωρητικές προσεγγίσεις οι οποίες χρησιμοποιούνται στο παρόν πόνημα ως οδηγός ερμηνείας των νομικών ρυθμίσεων που παρουσιάζονται.

Στο δεύτερο κεφάλαιο, αναλύεται το περιεχόμενο του όρου των οικονομικών δεδομένων, η σχέση του όρου με τα προσωπικά δεδομένα και οι διακρίσεις των οικονομικών δεδομένων, λαμβάνοντας ειδικότερα υπόψη τον παράγοντα της διασυνοριακής τους ροής.

Η έννοια της διασυνοριακής ροής των προσωπικών δεδομένων, στο περιβάλλον των κύριων τομέων που διέπουν τα οικονομικά δεδομένα, εξετάζεται στο τρίτο κεφάλαιο. Αναλυτικότερα, επιχειρείται η αποσαφήνιση της διασυνοριακής ροής των φορολογικών δεδομένων, των χρηματοοικονομικών δεδομένων και της διασυνοριακής ροής των δεδομένων στο πλαίσιο του διεθνούς εμπορίου. Στο ίδιο κεφάλαιο, εξετάζονται βασικά επιμέρους ζητήματα των οικονομικών δεδομένων με γνώμονα την ιδιωτικότητα, συντελώντας στην πολύπλευρη θέαση της διεθνούς διαβίβασής τους.

Το τέταρτο κεφάλαιο πραγματεύεται την παρουσίαση των επιπτώσεων της διακίνησης των προσωπικών δεδομένων στα ασύρματα δίκτυα 5ης γενιάς (5G) καθώς και στα αναδυόμενα δίκτυα 6ης γενιάς (6G). Πιο συγκεκριμένα, η συστηματική συσχέτιση των δικτύων 5ης γενιάς με την προστασία των προσωπικών δεδομένων σε ευρωπαϊκό επίπεδο αποσκοπεί στην ανάλυση των επιπτώσεων της καινοτόμας τεχνολογίας, λαμβάνοντας ειδικότερα την παράλληλη ανάπτυξη του Διαδικτύου των Πραγμάτων (IoT). Πέραν τούτου, στη δεύτερη ενότητα του τέταρτου κεφαλαίου περιλαμβάνεται η προσπάθεια ανάδειξης των καίριων ζητημάτων ιδιωτικότητας των δικτύων 6ης γενιάς και πιο συγκεκριμένα η ανάλυση του ρόλου της τεχνητής νοημοσύνης στο περιβάλλον αυτό, υπό το πρίσμα του ευρωπαϊκού δικαίου προστασίας των προσωπικών δεδομένων.

Στο πέμπτο κεφάλαιο, ολοκληρώνεται το πρώτο μέρος του πονήματος με την ανάδειξη της αντιμετώπισης των κρίσιμων ζητημάτων της προστασίας των προσωπικών δεδομένων των ανηλίκων, μέσω της σκοπιάς του ευρωπαϊκού δικαίου, σε σχέση με τις συσκευές IoT σε ένα έξυπνο οικιακό περιβάλλον (smart home), λαμβάνοντας υπόψη τα ζητήματα των διασυνοριακών ροών τα οποία ανακύπτουν.

Η νομική θεώρηση της διασυνοριακής ροής των δεδομένων, η οποία παρουσιάζεται στο Β΄ μέρος της διατριβής, εκκινεί με το έκτο κεφάλαιο. Αναλυτικότερα, στο έκτο κεφάλαιο επιχειρείται η συστηματική και διαχρονική ανάλυση των διεθνών ρυθμίσεων, οι οποίες διέπουν το πεδίο της διασυνοριακής ροής των δεδομένων, καθώς και η ταξινόμηση των εν λόγω νομικών ρυθμίσεων.

Το έβδομο κεφάλαιο περιλαμβάνει τις εθνικές ρυθμίσεις της διασυνοριακής ροής των δεδομένων σε παγκόσμιο επίπεδο, εξετάζοντας τις επιμέρους νομοθεσίες επιλεγμένων κρατών, όλων των γεωγραφικών ηπείρων, όσον αφορά το πεδίο της διασυνοριακής ροής των δεδομένων, προκειμένου να αναδειχθεί η σφαιρική προσέγγισή του.

Στο όγδοο κεφάλαιο, περιγράφονται οι ευρωπαϊκές ρυθμίσεις οι οποίες δύνανται να έχουν αντίκτυπο ή έχουν ως αντικείμενο την προστασία των προσωπικών δεδομένων. Η ανάλυση των παραμέτρων του όγδοου κεφαλαίου συντελείται με γνώμονα τη διασυνοριακή ροή των προσωπικών δεδομένων.

Στο ένατο κεφάλαιο, επιχειρείται η σκιαγράφηση των διατλαντικών ροών των προσωπικών δεδομένων, με άξονα τις μεταφορές δεδομένων από την ΕΕ στις ΗΠΑ, λαμβάνοντας ειδικότερα υπόψη τα οικονομικά δεδομένα. Η ανάλυση της διαχρονικής πορείας της διατλαντικής αυτής διαβίβασης, με την παράλληλη παρουσίαση των νεώτερων εξελίξεων, αποσκοπεί στην αποσαφήνιση του σημαντικού αυτού τομέα του πεδίου.

Αντικείμενο αναφοράς του δέκατου κεφαλαίου αποτελεί η περιγραφή της διασυνοριακής ροής των δεδομένων μεταξύ του Ηνωμένου Βασιλείου και της ΕΕ, μετά την αποχώρηση του πρώτου, επιδιώκοντας να προσεγγιστεί το σύγχρονο αυτό ζήτημα με βάση τις πρόσφατες εξελίξεις.

Η παρούσα διατριβή ολοκληρώνεται με τη διατύπωση συμπερασματικών παρατηρήσεων αλλά και προτάσεων για το σύγχρονο πλαίσιο των διασυνοριακών ροών των οικονομικών δεδομένων σε διεθνές επίπεδο. Η εκτίμηση των αποτελεσμάτων της διατριβής αποσκοπεί στην ενίσχυση του εξεταζόμενου πεδίου και στην επίλυση σύγχρονων ζητημάτων του.

ΜΕΡΟΣ Α΄

ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΟΙΚΟΝΟΜΙΚΩΝ ΔΕΔΟΜΕΝΩΝ:

ΟΝΤΟΛΟΓΙΚΗ ΘΕΩΡΗΣΗ

ΚΕΦΑΛΑΙΟ 1. ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΔΕΔΟΜΕΝΩΝ

1.1 Εννοιολογικός προσδιορισμός

Οι διασυνοριακές ροές δεδομένων περιγράφονται ως «οι διαβιβάσεις προσωπικών δεδομένων σε αποδέκτες αλλοδαπής δικαιοδοσίας».[5] Το πεδίο της «διασυνοριακής ροής δεδομένων» υπάγεται στον κλάδο του δικαίου των προσωπικών δεδομένων. Κατά τη δεκαετία του 1960, με την ανάπτυξη των δυνατοτήτων που παρείχαν οι ηλεκτρονικοί υπολογιστές, αναδείχθηκε το ζήτημα της προστασίας της ιδιωτικότητας και του απορρήτου, με συνέπεια τη θέσπιση των πρώτων εθνικών νόμων για την προστασία τους κατά τη δεκαετία του 1970.[6] Οι κατευθυντήριες γραμμές του ΟΟΣΑ από το 1980 αποτέλεσαν την απαρχή της θεσμοθέτησης σε διεθνές επίπεδο της έννοιας της «διασυνοριακής ροής δεδομένων».[7] [8]

Οι «διασυνοριακές ροές προσωπικών δεδομένων», σύμφωνα με τον ΟΟΣΑ, αποτελούν τις ροές προσωπικών δεδομένων εκτός των εθνικών συνόρων.[9] Αρχικοί ορισμοί της έννοιας της διασυνοριακής ροής δεδομένων την αποτύπωσαν ως «ηλεκτρονική διακίνηση δεδομένων μεταξύ των χωρών»[10] και ως «μετάδοση αναγνώσιμων δεδομένων και πληροφοριών μέσω υπερεθνικού υπολογιστή και άλλων συστημάτων ηλεκτρονικών επικοινωνιών για τους σκοπούς αποθήκευσης, ανάκτησης ή επεξεργασίας».[11]

Αναμφισβήτητα, σημείο καίριας σημασίας των ορισμών που περιγράφουν τη «διασυνοριακή ροή δεδομένων» αποτελεί η έννοια της «ροής»[12]. Ειδικότερα, το περιεχόμενο το οποίο αποδίδεται στον γενικό όρο «ροή» ή «διαβίβαση» των δεδομένων δύναται να διαφοροποιείται ανά δικαιοδοσία. Παράλληλα, ο τρόπος

[5] Αιτιολογική Έκθεση του τροποποιητικού Πρωτοκόλλου της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ατόμων σε σχέση με την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (223/2018), στοιχείο 102.

[6] Bigelow, R. (1979). Transborder data flow barriers. *Jurimetrics J.*, *20*, 8.

[7] Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, No. 187. OECD Publishing.

[8] Βλ. OECD (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[9] OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

[10] Fishman, W. L. (1980). Introduction to transborder data flows. *Stan. J. Int'l L.*, *16*, 1.

[11] Wigand, R. T., Shipley, C., & Shipley, D. (1984). Transborder data flow, informatics, and national policies. *Journal of Communication*, *34*(1), 153-175.

[12] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p.11.

με τον οποίο μπορεί να πραγματοποιηθεί μία διασυνοριακή διαβίβαση των δεδομένων εξαρτάται άμεσα από τις εκάστοτε δυνατότητες που προσφέρει η τεχνολογία ως προς την επεξεργασία των δεδομένων, καθιστώντας άρρηκτα συνδεδεμένο τον τομέα αυτόν της προστασίας των προσωπικών δεδομένων με την Επιστήμη της Πληροφορικής. Επιπρόσθετα, το περιεχόμενο του όρου «προσωπικά δεδομένα», τα οποία περιλαμβάνονται στις διεθνείς διαβιβάσεις, δύναται να διαφοροποιείται ανάλογα με τη νομοθεσία της κάθε χώρας[13].

Αναφορικά με την ανάγκη εξειδικευμένης προστασίας των προσωπικών δεδομένων στις διεθνείς διαβιβάσεις και συνακόλουθα την ανάπτυξη του συγκεκριμένου πεδίου, θα πρέπει να σημειωθεί ότι ήδη από νωρίς[14] [15] τέθηκε το ζήτημα της προστασίας των δεδομένων που διασχίζουν τα εθνικά σύνορα του κράτους του υποκειμένου των δεδομένων, το οποίο και εξακολουθεί[16] να αποτελεί τον επιδιωκόμενο στόχο του πεδίου.

Επιπρόσθετα, θα πρέπει να αναφερθεί ότι η θεσμοθέτηση της διασυνοριακής ροής δεδομένων κατ' ουσία διέπεται από περιορισμούς, χωρίς βέβαια αυτό να συνεπάγεται την εφαρμογή της προσέγγισης των πρώτων ετών, κατά την οποία η διασυνοριακή ροή δεδομένων αποτελούσε μία κατ' εξαίρεση συνθήκη[17]. Οι σύγχρονες επιταγές του οικονομικού και τεχνολογικού γίγνεσθαι έχουν πλέον αναδείξει την ανάγκη εφαρμογής εργαλείων με τα οποία πραγματοποιούνται οι διεθνείς διαβιβάσεις.

1.2 Προβληματισμοί/ προσεγγίσεις/σταθμίσεις στο πεδίο της διασυνοριακής ροής δεδομένων υπό το πρίσμα της προστασίας των προσωπικών δεδομένων

Η ακόλουθη ανάλυση των προσεγγίσεων και του είδους των εργαλείων που διέπουν τις διασυνοριακές ροές δεδομένων είναι χρήσιμη και με πρακτική σημασία για τη νομική θεώρηση του όρου στο Μέρος Β' και την προσπάθεια αποσαφήνισης του παγκόσμιου πλαισίου που τις διέπει.

---

[13] Βλ. Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287-344.

[14] Βλ. Αιτιολογική Έκθεση της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ατόμων σε σχέση με την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (108/1981), στοιχείο 8.

[15] Bigelow, R. (1979). Transborder data flow barriers. *Jurimetrics J.*, *20*, 8.

[16] «*Η διασυνοριακή διακίνηση δεδομένων προσωπικού χαρακτήρα εκτός της Ένωσης θέτει ενδεχομένως σε μεγαλύτερο κίνδυνο την ικανότητα των φυσικών προσώπων να ασκούν δικαιώματα προστασίας των δεδομένων*…» (Αιτιολογική σκέψη 116 GDPR).

[17] Βλ. Hondius, F. (1974). International Data Protection Action. In *Policy Issues in Data Protection and Privacy Policy Issues in Data Protection and Privacy*.

1.2.1 Οι προσεγγίσεις για τη ρύθμιση της διασυνοριακής ροής δεδομένων

Η θεσμοθέτηση των διασυνοριακών ροών των δεδομένων διακρίνεται σε δύο κύριες προσεγγίσεις. Η πρώτη προσέγγιση θέτει ως επίκεντρο την τοποθεσία και ειδικότερα τη χώρα εισαγωγής των δεδομένων, ενώ η δεύτερη προσέγγιση αφορά κυρίως στην υποχρέωση λογοδοσίας τόσο των εξαγωγέων όσο και των εισαγωγέων των προσωπικών δεδομένων σε επίπεδο οργανισμών[18]. Θα πρέπει, ωστόσο, να σημειωθεί ότι στοιχεία των δύο προσεγγίσεων μπορούν να ενυπάρχουν ταυτόχρονα σε μία νομοθεσία που διέπει τη διασυνοριακή ροή δεδομένων.

1) Προσέγγιση με βάση την τοποθεσία

Η γεωγραφική προσέγγιση στοχεύει στη σύγκριση των δικαιϊκών συστημάτων (ως προς την προστασία των προσωπικών δεδομένων) των χωρών, με στόχο τη διερεύνηση της ύπαρξης αντιστοίχου επιπέδου προστασίας. Η έννοια της επάρκειας της προστασίας των προσωπικών δεδομένων αποτελεί κεντρικό στοιχείο της εν λόγω προσέγγισης[19], απορρέοντας από τις ρυθμίσεις (Οδηγία 95/46/ΕΚ και GDPR) του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Ωστόσο, η αξιολόγηση της δυνατότητας της διαβίβασης των δεδομένων μόνο με βάση τη νομοθεσία της τρίτης χώρας δύναται να παραγκωνίσει άλλους παράγοντες που μπορεί να επηρεάσουν την εκάστοτε διαβίβαση και δεν αποτυπώνονται στους νόμους της.

2) Προσέγγιση με βάση τους οργανισμούς

Η προσέγγιση αυτή εστιάζει στην υποχρέωση λογοδοσίας του εξαγωγέα των δεδομένων και ειδικότερα στη συνεχιζόμενη και αδιάκοπη προστασία των προσωπικών δεδομένων μετά τη διαβίβασή τους. Οι μηχανισμοί των διασυνοριακών ροών στο πλαίσιο της οικονομικής συνεργασίας Ασίας-Ειρηνικού (APEC)[20], φαίνεται ότι διαπνέονται από τους προαναφερθέντες άξονες της προσέγγισης στην παρ. 65 και 69. Η έννοια της λογοδοσίας έχει ως αποτέλεσμα και την αναζήτηση των κατάλληλων μέτρων για τη διασυνοριακή ροή των δεδομένων από την πλευρά των εν δυνάμει εξαγωγέων των δεδομένων. Αναλυτικότερα, οι δύο ευρωπαϊκοί μηχανισμοί διασυνοριακών διαβιβάσεων, των

[18] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p.64-76.

[19] Weber, R. H. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, *3*(2), 117-130.

[20] APEC. (2015). APEC Privacy Framework. Singapore: APEC. Διαθέσιμο στο: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

τυποποιημένων ρητρών προστασίας δεδομένων και των δεσμευτικών εταιρικών κανόνων, αποτελούσαν (όπως ίσχυαν και πριν τη θέση σε εφαρμογή του GDPR) και αποτελούν εκφάνσεις αυτής της προσέγγισης[21]. Παράλληλα, ενίσχυση της υποχρέωσης λογοδοσίας των υπευθύνων της διασυνοριακής ροής δεδομένων στον ευρωπαϊκό χώρο αποτελεί η υποχρέωση που έθεσε το ΔΕΕ στην υπόθεση C-311/18 (Schrems II) για την εφαρμογή πρόσθετων μέτρων, όταν απαιτείται, στην περίπτωση των τυποποιημένων ρητρών προστασίας δεδομένων[22].

Ως προς το είδος των εργαλείων στα οποία μπορούν να βασιστούν οι διασυνοριακές ροές δεδομένων, ιδιαίτερα μέσα από το πρίσμα μίας οντότητας η οποία θέλει να εξαγάγει δεδομένα, καταγράφονται 4 κατηγορίες στην πρόσφατη Έκθεση[23] του ΟΟΣΑ στο πλαίσιο της Συνόδου των G20. Πιο συγκεκριμένα, τα εργαλεία των διασυνοριακών ροών διακρίνονται σε: πολυμερείς ρυθμίσεις, εμπορικές συμφωνίες, μονομερείς ρυθμίσεις και εργαλεία του ιδιωτικού τομέα σε συνδυασμό με άλλες πρωτοβουλίες.

1) Πολυμερείς ρυθμίσεις

Οι πολυμερείς συμφωνίες στοχεύουν στη σύγκλιση μεταξύ πολλών χωρών σχετικά με τις διασυνοριακές διαβιβάσεις, με δεσμευτικό ή όχι νομικό χαρακτήρα[24]. Οι *κατευθυντήριες γραμμές του ΟΟΣΑ για την προστασία της ιδιωτικής ζωής και τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα* από το 1980 και η *Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα* του 1981 του Συμβουλίου της Ευρώπης αποτελέσαν τις πρώτες διεθνείς πολυμερείς ρυθμίσεις και αναλύονται εκτενέστερα στο κεφάλαιο 6.

2) Εμπορικές συμφωνίες

[21] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p.64-76.

[22] C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems, σκέψη 134.

[23] OECD. (2020). Mapping approaches to cross-border data flows. Report for the G20 Digital Economy Task Force. Διαθέσιμο στο: https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1620464835&id=id&accname=guest&checksum=BCE1CCC78F3747D1386E1D0446E3B8CC

[24] OECD. (2020). Mapping approaches to cross-border data flows. Report for the G20 Digital Economy Task Force. Διαθέσιμο στο: https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1620464835&id=id&accname=guest&checksum=BCE1CCC78F3747D1386E1D0446E3B8CC

Οι εμπορικές συμφωνίες, ειδικότερα μέσα στο περιβάλλον της σύγχρονης ψηφιακής οικονομίας, μπορούν να αποτελέσουν μοχλό στη διασυνοριακή ρύθμιση των ροών, κυρίως των οικονομικών δεδομένων. Η *Συνολική και Προοδευτική Συμφωνία για την Εταιρική Σχέση των Χωρών του Ειρηνικού (CPTPP)*[25]**,** η οποία αναλύεται εκτενέστερα στο κεφάλαιο 6, αποτελεί παράδειγμα εμπορικής συμφωνίας με ρυθμιστικό πλαίσιο των διασυνοριακών ροών.

3) Μονομερείς ρυθμίσεις

Στην κατηγορία αυτή ανήκουν οι εθνικές ρυθμίσεις των διασυνοριακών διαβιβάσεων και περιλαμβάνονται όλοι οι διαθέσιμοι τρόποι-εργαλεία τα οποία θεσπίζονται, αντικατοπτρίζοντας και το επίπεδο στο οποίο βρίσκεται μία χώρα ως προς την προστασία των προσωπικών δεδομένων.

4) Εργαλεία του ιδιωτικού τομέα σε συνδυασμό με άλλες πρωτοβουλίες

Σε αυτήν την κατηγορία υπάγονται εργαλεία, τα οποία απευθύνονται κυρίως σε οικονομικές οντότητες και δύνανται να δράσουν συμπληρωματικά στην προσπάθεια συμμόρφωσης με το νομικό πλαίσιο, το οποίο θα πρέπει να ακολουθηθεί για τις διεθνείς διαβιβάσεις. Περιλαμβάνει διεθνή πρότυπα και τεχνολογίες, όπως το πρότυπο ISO[26] και οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies, PETs)[27], οι οποίες στοχεύουν στην προστασία της ιδιωτικότητας από τον σχεδιασμό[28].

1.2.2 Η προσέγγιση του δικαιώματος της προστασίας των προσωπικών δεδομένων σε ΕΕ και ΗΠΑ

Αναμφισβήτητα, οι κανόνες που διέπουν τη διασυνοριακή ροή των δεδομένων αντανακλούν τη θέση του δικαιώματος της προστασίας των προσωπικών δεδομένων στο δικαιϊκό σύστημα στο οποίο ανήκουν αυτοί οι κανόνες.

[25] López-González, J., Casalini, F., & Nemoto, T. (2021). Mapping approaches to cross-border data flows. *Addressing Impediments to Digital Trade*.

[26] Βλ. ISO/IEC 27701:2019. Security techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirements and guidelines. Διαθέσιμο στο: https://www.iso.org/standard/71670.html

[27] López-González, J., Casalini, F., & Nemoto, T. (2021). Mapping approaches to cross-border data flows. *Addressing Impediments to Digital Trade*.

[28] Βλ. Μήτρου, Λ. (2010). Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών.* Αθήνα: Παπασωτηρίου, σελ. 505-552.

Το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν είναι ένα απόλυτο δικαίωμα[29] [30] [31] [32], γεγονός που σημαίνει ότι ο περιορισμός αυτού του δικαιώματος θα μπορούσε να επιτραπεί υπό συγκεκριμένες περιστάσεις (π.χ. δημόσιο συμφέρον, υπερισχύοντα συμφέροντα ή θεμελιώδη δικαιώματα). Ωστόσο, οι σταθμίσεις που επιβάλλονται στον οποιοδήποτε περιορισμό του είναι αυτές που καθορίζουν και το ίδιο το δικαίωμα, αλλά και την αποτελεσματικότητα των εργαλείων της διασυνοριακής ροής των δεδομένων.

1.2.2.1 Η προσέγγιση της ΕΕ

Καταρχάς, ως προς τον όρο που χρησιμοποιείται ως επί το πλείστον στην ΕΕ, το δικαίωμα καταγράφεται ως δικαίωμα στην προστασία των προσωπικών δεδομένων[33]. Η προστασία των προσωπικών δεδομένων κατέχει τη θέση του θεμελιώδους δικαιώματος στην ενωσιακή έννομη τάξη[34], θεσπιζόμενο στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ[35] και στο άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης[36].

Το νομοθετικό πλαίσιο, στο οποίο τοποθετείται το δικαίωμα στην προστασία των προσωπικών δεδομένων στην ΕΕ και το οποίο αναλύεται στο

[29] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Αιτιολογική σκέψη 4. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[30] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα, σελ. 19.

[31] Bottis, M., Panagopoulou-Koutnatzi, F., Michailaki, A., & Nikita, M. (2019). The right to access information under the GDPR. *International Journal of Technology Policy and Law*, *3*(2), 131-142.

[32] Ventrella, E. (2020). Privacy in emergency circumstances: data protection and the COVID-19 pandemic. In *ERA Forum* (Vol. 21, No. 3, pp. 379-393). Springer Berlin Heidelberg.

[33] Patel, O., & Lea, N. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. *Available at SSRN 3618937*.

[34] Βλ. https://www.europarl.europa.eu/about-parliament/el/democracy-and-human-rights/fundamental-rights-in-the-eu/adapting-to-the-digital-age

[35] Βλ. Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης *ΕΕ C 202 της 7.6.2016.* Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016P%2FTXT

[36] Βλ. Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης *ΕΕ C 326 της 26.10.2012.* Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:12012E/TXT

κεφάλαιο 8, στοχεύει στην εναρμόνιση των δικαίων των κρατών-μελών και στην ενιαία ρύθμιση που πρέπει να διέπει αναλυτικά όλο το φάσμα των τομέων του κοινωνικοοικονομικού γίγνεσθαι.

1.2.2.2 Η προσέγγιση των ΗΠΑ

Στις ΗΠΑ γίνεται ευρύτερη χρήση του όρου της «προστασίας της ιδιωτικότητας»[37] και δεν κατοχυρώνεται η αναγνώριση της ως θεμελιώδους δικαιώματος. Αναλυτικότερα, ενώ δεν υπάρχει συνταγματική αναφορά του δικαιώματος στην ιδιωτικότητα[38], το Ανώτατο Δικαστήριο των ΗΠΑ αναγνώρισε από την απόφαση *Griswold v. Connecticut* το 1965 το δικαίωμα στην ιδιωτική ζωή με μία διασταλτική ερμηνεία της 9ης Τροποποίησης του Συντάγματος, με τη διαχρονική στάση απέναντι στο δικαίωμα να διαμορφώνεται ως ελευθερία απέναντι στο κράτος και όχι κατά άλλων πολιτών [39].

Η προσέγγιση των ΗΠΑ απέναντι στο θεσμικό πλαίσιο που διέπει την ιδιωτικότητα αποτελείται από ένα σύνολο νομοθετικών πράξεων, κανονιστικών διατάξεων και διατάξεων αυτορρύθμισης οι οποίες ρυθμίζουν, ως επί το πλείστον, έναν συγκεκριμένο τομέα[40]. Αναλυτικότερα, η τομεακή ρύθμιση αναφέρεται στην ύπαρξη εξειδικευμένων νόμων για την προστασία της ιδιωτικότητας, με παραδείγματα τον νόμο *Gramm-Leach Bliley Act,* ο οποίος διέπει τα προσωπικά δεδομένα στον χρηματοοικονομικό τομέα[41], τον νόμο *Health Insurance Portability and Accountability Act* (HIPAA), ο οποίος διέπει τα προσωπικά δεδομένα υγείας[42], τις ρυθμίσεις για την τεχνολογία R.F.I.D (Radio Frequency

[37] Patel, O., & Lea, N. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. *Available at SSRN 3618937*.

[38] Patel, O., & Lea, N. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. *Available at SSRN 3618937*.

[39] Βλ. Κανελλοπούλου-Μπότη, Μ. (2009). Η προστασία της ιδιωτικής ζωής και η ευρωπαϊκή νομοθεσία για τα προσωπικά δεδομένα-σκέψεις σε σχέση με την προστασία της ιδιωτικής ζωής στις ΗΠΑ στον *Τιμητικό Τόμο Μιχ. Π. Σταθόπουλου, τόμος ΙΙ*. εκδ. Αντ.Ν. Σάκκουλα. Αθήνα-Κομοτηνή, σελ.809-823. Διαθέσιμο στο: http://bottis.ihrc.gr/en/publications/2009/

[40] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων). *ΔΙΜΕΕ, 1*, 12-24.

[41] McGeveran, W., & Schmitz, C. (2020). General-Purpose Privacy Regulation and Translational Genomics. *The Journal of Law, Medicine & Ethics*, *48*(1), 142-150.

[42] Gerke, S., Shachar, C., Chai, P. R., & Cohen, I. G. (2020). Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nature medicine*, *26*(8), 1176-1182.

Identification, «ταυτοποίηση μέσω ραδιοσυχνοτήτων»)[43] και τέλος τον νόμο για την προστασία της ιδιωτικότητας των παιδιών στο Διαδίκτυο (Children's Online Privacy Protection Rule, COPPA)[44]. Εντούτοις, έχει υποστηριχθεί[45] ότι η τομεακή στάση των ΗΠΑ απέναντι στην ιδιωτικότητα εξυπηρετεί τον συγχρονισμό με τις τεχνολογικές εξελίξεις στον κάθε τομέα δραστηριοτήτων λόγω της δυνατότητας άμεσης τροποποίησης της νομοθεσίας.

Παράλληλα, θα πρέπει να αναφερθεί ότι το μοντέλο προστασίας της ιδιωτικότητας των ΗΠΑ έχει χαρακτηριστεί ως ένα μοντέλο που εδράζεται στην «προστασία των καταναλωτών»[46]. Μια άλλη προσέγγιση στο μοντέλο των ΗΠΑ για την ιδιωτικότητα τονίζει ότι το θεσμικό πλαίσιο των ΗΠΑ διαπνέεται από τη διαχρονική ανάγκη ανάδειξης της αξίας της ατομικής ελευθερίας σε αντιδιαστολή με το πλαίσιο της ΕΕ στο οποίο βαρύνει η αξία της ανθρώπινης αξιοπρέπειας και του δικαιώματος στον αυτοκαθορισμό[47]. Επιπροσθέτως, ιδιαίτερα μετά τις τρομοκρατικές επιθέσεις που βίωσαν οι ΗΠΑ το 2001, στο επίκεντρο τέθηκε η εθνική ασφάλεια, η οποία έχει υπερτερήσει στη στάθμιση με το δικαίωμα της προστασίας της ιδιωτικότητας[48] [49]. Ειδικότερα, το ζήτημα αυτό, και ιδιαίτερα σε ό,τι αφορά τον αντίκτυπό του στα προσωπικά δεδομένα Ευρωπαίων πολιτών, αποτέλεσε το αντικείμενο των συμφωνιών PNR και SWIFT[50], οι οποίες αναλύονται στο κεφάλαιο 9.

[43] Αλεξανδροπούλου-Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η προστασία των προσωπικών δεδομένων ενόψει της εφαρμογής της νέας τεχνολογίας της ταυτοποίησης με ραδιοσυχνότητες (R.F.I.D.) – Νομική και τεχνολογική προσέγγιση. *Αρμενόπουλος, 4*, 493-504.

[44] Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2007). Η πλοήγηση των ανηλίκων στο Διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων. *Αρμενόπουλος, 6*, 848-854.

[45] Schwartz, P. M. (2008). Preemption and privacy. *Yale Lj*, *118*, p. 902-947.

[46] McGeveran, W., & Schmitz, C. (2020). General-Purpose Privacy Regulation and Translational Genomics. *The Journal of Law, Medicine & Ethics*, *48*(1), 142-150.

[47] Whitman, J. Q. (2003). The two western cultures of privacy: Dignity versus liberty. *Yale LJ*, *113*, 1151.

[48] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων). *ΔΙΜΕΕ, 1*, 12-24.

[49] Patel, O., & Lea, N. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. *Available at SSRN 3618937*.

[50] Βλ. Martina, D. (2017). EU-USA cooperation on information sharing in the fight against terrorism: the roles of privacy and security, and the cases of the TFTP and PNR agreements.

ΚΕΦΑΛΑΙΟ 2. ΟΙΚΟΝΟΜΙΚΑ ΔΕΔΟΜΕΝΑ

2.1 Εννοιολογικός προσδιορισμός

Τα δεδομένα γενικά συνίστανται σε γεγονότα ή πληροφορίες, τα οποία, ειδικότερα, εξετάζονται και χρησιμοποιούνται για την αποκάλυψη πραγμάτων ή τη λήψη αποφάσεων.[51]

Τα οικονομικά δεδομένα περιλαμβάνουν ένα ευρύ περιεχόμενο στοιχείων τα οποία μπορούν να συγκροτούνται από πληροφορίες σχετιζόμενες με οποιαδήποτε οικονομική δραστηριότητα ή κατάσταση. Οι υπηρεσίες του χρηματοοικονομικού τομέα, αποτελούν έναν από τους τομείς που δέχονται τον μεγαλύτερο όγκο δεδομένων[52], στα οποία ενυπάρχουν και προσωπικά δεδομένα. Τα οικονομικά δεδομένα, εξεταζόμενα υπό το πρίσμα της προστασίας των προσωπικών δεδομένων στην παρούσα εργασία, θα πρέπει να διακριθούν σε προσωπικά και μη προσωπικά δεδομένα.

Καταρχάς, όσον αφορά τον ορισμό των προσωπικών δεδομένων, σύμφωνα με τον ΟΟΣΑ, αποτελούν «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*»[53] και ομοίως σύμφωνα με τον GDPR «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*»[54].

[51] Βλ. https://www.oxfordlearnersdictionaries.com/definition/english/data

[52] OECD. (2015). *Data-driven innovation: Big data for growth and well-being*.

[53] OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Annex, Part 1, definitions. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

[54]Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Άρθρο 4 περ.1. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Παράλληλα, σχετικά με τη διάκριση των προσωπικών και μη προσωπικών οικονομικών δεδομένων, αυτή αφορά όχι μόνο την εννοιολογική διαφοροποίησή τους αλλά και τον βαθμό της δυνατότητας των σύγχρονων τεχνικών ανάλυσης δεδομένων να μετατρέπουν τα μη προσωπικά δεδομένα σε προσωπικά[55] ως επιπρόσθετο στοιχείο διάκρισής τους. Πιο συγκεκριμένα, αν είναι εφικτή αυτή η διαδικασία μετατροπής, λαμβάνοντας υπόψη τα σύγχρονα τεχνολογικά μέσα[56], τότε τα δεδομένα θεωρούνται προσωπικά και υπόκεινται στη νομοθεσία για την προστασία των δεδομένων.

Η υποκατηγορία των οικονομικών δεδομένων, τα οποία θεωρούνται προσωπικά δεδομένα, είναι τα προσωπικά δεδομένα οικονομικής συμπεριφοράς. Τα προσωπικά δεδομένα οικονομικής συμπεριφοράς[57] [58] [59] [60] συνίστανται στα οικονομικά στοιχεία[61] του ατόμου τα οποία απορρέουν από το δικαίωμα της πληροφορικής του αυτοδιάθεσης[62]. Τα προσωπικά δεδομένα οικονομικής συμπεριφοράς μπορούν να περιλαμβάνουν στοιχεία τόσο της οικονομικής όσο και της κοινωνικής ζωής του ατόμου, όπως οι πληροφορίες σχετικά με την επαγγελματική ζωή του ατόμου. Ενδεικτικά, στα κύρια χρηματοοικονομικά στοιχεία του ατόμου θα μπορούσαν να περιληφθούν: τα στοιχεία τραπεζικών

[55]OECD (2013). *Introduction to Data and Analytics (Module 1): Taxonomy, Data Governance Issues, and Implications for further Work*.

[56]Βλ. Αιτιολογική σκέψη 26 GDPR.

[57]Βλ. Σαατζίδου-Παντελιάδου, Ε. (2006). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας: το παράδειγμα της νομικής ρύθμισης της ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς, σελ.143 κ. επ.

[58]Βλ. Μυλώση, Μ., Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2015). Προσωπικά δεδομένα οικονομικής συμπεριφοράς και η ηλεκτρονική επεξεργασία τους από την Τειρεσίας Α.Ε. *ΔΙΜΕΕ, 1*, σελ. 25 κ. επ.

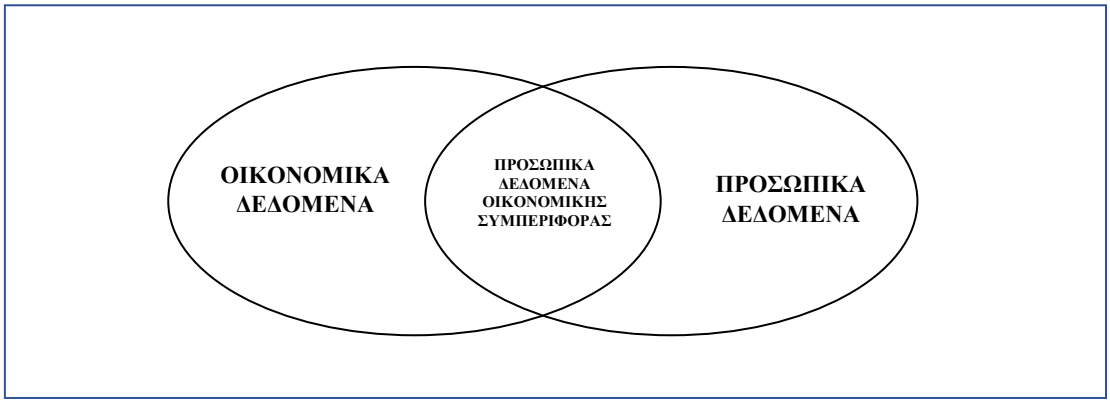
[59]Βλ. Μυλώση, Μ. (2015). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία, σελ. 5 κ. επ.

[60]Βλ. Χριστοδούλου, Κ. (2020). *Δίκαιο Προσωπικών Δεδομένων*. Εκδ. Νομική Βιβλιοθήκη, σελ. 195 κ. επ.

[61]Ο όρος «οικονομικά στοιχεία» περιλαμβάνεται στην διάκριση των ειδών των προσωπικών δεδομένων στην Φόρμα γνωστοποίησης περιστατικού παραβίασης στην Αρχή (άρθρο 33 ΓΚΠΔ) στην ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Διαθέσιμο στο: https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis/upovoli_gnwstopoihshs_paraviashs

[62]Σαατζίδου-Παντελιάδου, Ε. (2006). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας: το παράδειγμα της νομικής ρύθμισης της ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς, σελ.143.

λογαριασμών, τα στοιχεία ιδιοκτησίας, οι συναλλαγές και τα στοιχεία της πιστοληπτικής ικανότητας του ατόμου[63].



Εικόνα 1. Η σχέση των οικονομικών δεδομένων με τα προσωπικά δεδομένα

2.2 Διακρίσεις των οικονομικών δεδομένων

Η πρακτική σημασία της διάκρισης των οικονομικών δεδομένων, στα οποία δύνανται να περιλαμβάνονται προσωπικά δεδομένα, έγκειται στην καλύτερη ανάδειξη των ζητημάτων ιδιωτικότητας που εγείρουν, ιδιαίτερα υπό το πρίσμα των οικονομικών οντοτήτων, στην προσπάθεια της μέτρησης του οικονομικού αντικτύπου[64] των προσωπικών δεδομένων, αλλά και στο πλαίσιο της διασυνοριακής διαβίβασής τους.

Υπό το πρίσμα των επιχειρήσεων, τα δεδομένα τα οποία γίνονται αντικείμενο επεξεργασίας με βάση τον τρόπο χρήσης τους είναι: τα εταιρικά δεδομένα (πχ. χρηματοοικονομικά στοιχεία), τα δεδομένα πελατών (πχ. στοιχεία συναλλαγών, στοιχεία πιστοληπτικής ικανότητας), τα δεδομένα που αφορούν το ανθρώπινο δυναμικό της οικονομικής οντότητας, τα εμπορικά δεδομένα (στοιχεία προμηθευτών και άλλων οικονομικών οντοτήτων) και τα δεδομένα που αφορούν

[63] Enterprivacy Consulting Group. (2017). Categories of Personal Information. Διαθέσιμο στο: https://iapp.org/resources/article/categories-of-personal-data/

[64] Βλ. Nguyen, D., & Paczos, M. (2020). Measuring the economic value of data and cross-border data flows: A business perspective. Διαθέσιμο στο: https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en

τεχνικά χαρακτηριστικά των προϊόντων ή των υπηρεσιών της οικονομικής οντότητας.[65]

Μια ειδικότερη κατηγοριοποίηση των οικονομικών δεδομένων, η οποία λαμβάνει υπόψη και τις διασυνοριακές ροές των δεδομένων, είναι η κατηγοριοποίηση του Υπουργείου Εμπορίου των Η.Π.Α.[66] Ειδικότερα, ως δεδομένα των οποίων η διασυνοριακή ροή επιφέρει οικονομικές επιπτώσεις παρατίθενται τα ακόλουθα:

- Δεδομένα αποκλειστικά μη εμπορικά, όπως κυβερνητικά ή στρατιωτικά δεδομένα.
- Δεδομένα που αφορούν συναλλαγές, όπως διαδικτυακές τραπεζικές υπηρεσίες ή πωλήσεις.
- Εμπορικά δεδομένα και υπηρεσίες που ανταλλάσσονται μεταξύ ή εντός επιχειρήσεων και άλλων μερών, όπως τα δεδομένα του ανθρώπινου δυναμικού και τα δεδομένα της εφοδιαστικής αλυσίδας.
- Ψηφιακά δεδομένα και υπηρεσίες απευθυνόμενα σε χρήστες, όπως τα δεδομένα των κοινωνικών μέσων δικτύωσης και η ηλεκτρονική αλληλογραφία.

Οι προαναφερθείσες διακρίσεις, οι οποίες εστιάζουν στα οικονομικά δεδομένα, αποβλέπουν κυρίως στη μετάφραση των δεδομένων και των ροών των δεδομένων σε οικονομική αξία[67]. Για το πλαίσιο της προστασίας της ιδιωτικότητας οι παραπάνω διακρίσεις μπορούν να καταδείξουν τα κύρια δεδομένα, τα οποία βρίσκονται στο επίκεντρο του ενδιαφέροντος για τις οικονομικές οντότητες και τους διεθνείς οργανισμούς[68] και τα οποία δύνανται να αποτελέσουν το αντικείμενο των μηχανισμών των διασυνοριακών ροών.

---

[65] Swedish National Board of Trade. (2014). No Transfer, No Trade– the Importance of Cross-Border Data Transfers for Companies Based in Sweden. Διαθέσιμο στο: https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf

[66] Nicholson, J.R., & Noonan, R. (2014). Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services. U.S. Department of Commerce. Διαθέσιμο στο: https://www.commerce.gov/sites/default/files/migrated/reports/digitaleconomyandcross-bordertrade.pdf

[67] Βλ. US Department of Commerce. (2016). Measuring the Value of Cross-Border Data Flows. Διαθέσιμο στο: https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf

[68] Βλ. Nguyen, D., & Paczos, M. (2020). Measuring the economic value of data and cross-border data flows: A business perspective. Διαθέσιμο στο: https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en

2.3 Νομική φύση των οικονομικών δεδομένων ως προσωπικών δεδομένων

Το ευρωπαϊκό πλαίσιο προστασίας των προσωπικών δεδομένων διαχρονικά, τόσο στην Οδηγία 95/46/ΕΚ, αλλά και στον GDPR, αναγνωρίζει δύο μόνο κατηγορίες προσωπικών δεδομένων, ήτοι τις «ειδικές κατηγορίες προσωπικών δεδομένων» ή ευαίσθητα δεδομένα και τα απλά προσωπικά δεδομένα.[69]

Η πρακτική σημασία για την υπαγωγή των προσωπικών δεδομένων στη μία ή στην άλλη κατηγορία έχει πολλαπλές επιπτώσεις στο επίπεδο προστασίας τους[70]. Αναλυτικότερα, για την οποιαδήποτε επεξεργασία ευαίσθητων δεδομένων θα πρέπει να υφίσταται αφενός μία νόμιμη βάση επεξεργασίας (Άρθρο 6 και Άρθρο 9 GDPR). Επιπλέον, στην περίπτωση της αυτοματοποιημένης λήψης αποφάσεων, μαζί με την ικανοποίηση των εξαιρέσεων του άρθρου 22 GDPR, θα πρέπει να εφαρμόζεται μία από τις περιπτώσεις του άρθρου 9 παρ. 2 στοιχείο α ή ζ. Ακόμη, η διαφοροποίηση των δύο κατηγοριών εμφανίζεται στην υποχρεωτική διενέργεια εκτίμησης αντικτύπου, όταν υφίστανται επεξεργασία μεγάλης κλίμακας[71] (Άρθρο 35 παρ. 3 περ. β GDPR) και στην υποχρέωση ορισμού υπεύθυνου προστασίας των δεδομένων (Άρθρο 37 παρ. 1 περ. γ GDPR).

Αξίζει να σημειωθεί ότι παρά το γεγονός ότι τα οικονομικά δεδομένα δεν περιλαμβάνονται στα ευαίσθητα δεδομένα[72] (*που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό* [Άρθρο 9 παρ. 1 GDPR]), όχι μόνο από την ευρωπαϊκή νομοθεσία, αλλά και από τη διεθνή[73], εντούτοις ο χρηματοοικονομικός τομέας συγκεντρώνει από τα

[69] Cradock, E., Stalla-Bourdillon, S., & Millard, D. (2017). Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform. *Computer law & security review*, *33*(2), 142-158.

[70] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 52.

[71] Βλ. ΑΠΔΠΧ. Απόφαση Αριθ. 65/2018. (ΦΕΚ 1622/Β/10-5-2019). Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.

[72] Παπακωνσταντίνου, Ε. (2010). *Δίκαιο πληροφορικής*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 163.

[73] Wang, M., & Jiang, Z. (2017). The defining approaches and practical paradox of sensitive data: An investigation of data protection laws in 92 countries and regions and 200 data breaches in the world. *International Journal of Communication*, *11*, 20.

υψηλότερα περιστατικά παραβιάσεων δεδομένων σε σχέση με τους άλλους τομείς.[74]

Ωστόσο, για την αξιολόγηση της ρύθμισης των οικονομικών στοιχείων του ατόμου ως μη ευαίσθητα θα πρέπει να εκκινήσουμε από τα κριτήρια υπαγωγής των δεδομένων στην κατηγορία των ευαίσθητων προσωπικών δεδομένων. Αναλυτικότερα, η ειδική ρύθμιση των ευαίσθητων δεδομένων έχει ως στόχο την προστασία των ατόμων από το να υποστούν διακρίσεις σε βάρος τους, ως απόρροια ορισμένων μόνο στοιχείων της ταυτότητάς τους (πολιτικής, θρησκευτικής, φυλετικής κ.α.) και όχι της συνολικής προσωπικότητάς τους[75] [76]. Όσον αφορά την αντίληψη της κοινωνίας για τα οικονομικά δεδομένα του ατόμου, μεγάλη μερίδα τα αντιλαμβάνεται ως ευαίσθητα[77]. Παράλληλα, κάποια στοιχεία των οικονομικών δεδομένων θα μπορούσαν να οδηγήσουν στην δημιουργία διακρίσεων σε βάρος του ατόμου. Εξάλλου, η περιουσία του ατόμου αποτελεί, κατά το άρθρο 14 της ΕΣΔΑ, πεδίο ανάπτυξης διακρίσεων[78]. Παράδειγμα που δεν πρέπει να αγνοηθεί αποτελεί η δυνατότητα λήψης απόφασης από ένα χρηματοπιστωτικό ίδρυμα για την πιστοληπτική ικανότητα του εκάστοτε ατόμου, μέσω του συστήματος «ΤΕΙΡΕΣΙΑΣ», που θα μπορούσε να οδηγήσει ως μόνο στοιχείο στην κατάταξή του[79]. Στον αντίποδα, όπως υποστηρίζεται[80], στη στάθμιση της θέσπισης των οικονομικών δεδομένων ως ευαίσθητων, το βάρος πέφτει στην ανάγκη διαφάνειας και περιορισμού των οικονομικών εγκλημάτων.

Καταλήγοντας, εφόσον τα οικονομικά δεδομένα δεν έχουν τεθεί ως ευαίσθητα, και ίσως η διεύρυνση του καταλόγου των ευαίσθητων δεδομένων θα επέφερε δυσανάλογες εξαιρέσεις στην επεξεργασία τους, η αναβάθμιση του

---

[74]Βλ.Verizon. (2020) Data Breach Investigations Report. Διαθέσιμο στο: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[75] Βλ. Ιγγλεζάκης, Ι. (2003). *Ευαίσθητα προσωπικά δεδομένα*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 114 κ. επ.

[76] Βλ. Πρωτοπαπαδάκης, Ε. Δ. (2016). *Προσωπικά δεδομένα: Μια ηθική προσέγγιση* σε Κοτσαλής Λ. (επιμ.) *Προσωπικά δεδομένα (Ανάλυση - Σχόλια - Εφαρμογή)*. Νομική Βιβλιοθήκη, σελ. 452.

[77] Βλ. Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2007). Προσωπικά δεδομένα (Νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους). Εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή, σελ. 37.

[78] *Η χρήσις των αναγνωριζομένων εν τη παρούση Συμβάσει δικαιωμάτων και ελευθεριών δέον να εξασφαλισθή ασχέτως διακρίσεως φύλου, φυλής, χρώματος, γλώσσης, θρησκείας, πολιτικών ή άλλων πεποιθήσεων, εθνικής ή κοινωνικής προελεύσεως, συμμετοχής εις εθνικήν μειονότητα, περιουσίας, γεννήσεως ή άλλης καταστάσεως.* (Άρθρο 14 ΕΣΔΑ)

[79] Βλ. Μυλώση, Μ., Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2015). Προσωπικά δεδομένα οικονομικής συμπεριφοράς και η ηλεκτρονική επεξεργασία τους από την Τειρεσίας Α.Ε. *ΔΙΜΕΕ, 1*, σελ. 26.

[80] Βλ. Ιγγλεζάκης, Ι. (2003). *Ευαίσθητα προσωπικά δεδομένα*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 94.

καθεστώτος των οικονομικών δεδομένων διαφαίνεται ότι επέρχεται μέσω των μέτρων ασφαλείας. Ειδικότερα, θα πρέπει να αναφερθεί ότι τα οικονομικά δεδομένα τοποθετούνται στην ίδια κατηγοριοποίηση με τα ευαίσθητα δεδομένα, ως κατηγορία δεδομένων των οποίων η επεξεργασία απαιτεί διεξαγωγή εκτίμησης αντικτύπου λόγω υψηλών κινδύνων[81]. Επιπρόσθετα, τα οικονομικά δεδομένα της «οικονομικής κατάστασης» και της «πιστοληπτικής ικανότητας» τίθενται από την ΑΠΔΠΧ στην πρώτη κατηγορία με τα είδη και τους σκοπούς της επεξεργασίας για τα οποία απαιτείται η διενέργεια εκτίμησης αντικτύπου[82], πριν την επεξεργασία τους. Αυτή η ρύθμιση έρχεται σε αντιστοιχία αφενός με το οικονομικό κόστος και την συχνότητα των παραβιάσεων των οικονομικών διδομένων και αφετέρου με την ανάγκη επιπρόσθετης ευαισθητοποίησης και επαγρύπνησης, κυρίως από τους χρηματοπιστωτικούς οργανισμούς, σχετικά με την ιδιωτικότητα των οικονομικών στοιχείων του ατόμου.

[81] Βλ. Ομάδα Εργασίας του Άρθρου 29. (2017). "Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679". Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/611236

[82] Βλ. ΑΠΔΠΧ. Απόφαση Αριθ. 65/2018. (ΦΕΚ 1622/Β/10-5-2019). Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.

ΚΕΦΑΛΑΙΟ 3. Η ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΤΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΓΕΝΙΚΟ ΡΥΘΜΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΜΕ ΕΜΦΑΣΗ ΣΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

3.1 Εισαγωγή

Στο κεφάλαιο αυτό θα εξεταστεί η έννοια της διασυνοριακής ροής των προσωπικών δεδομένων υπό το πρίσμα των κύριων τομέων που διέπουν τα οικονομικά δεδομένα. Ειδικότερα, αναλύεται η διασυνοριακή ροή των φορολογικών δεδομένων, των χρηματοοικονομικών δεδομένων και η διασυνοριακή ροή των δεδομένων στο διεθνές εμπόριο.

3.2 Η διασυνοριακή ροή των φορολογικών δεδομένων

Οι διασυνοριακές ροές των φορολογικών δεδομένων σε παγκόσμιο επίπεδο συντελούνται με σκοπό τον περιορισμό των φαινομένων της φοροδιαφυγής, της φοροαποφυγής, ειδικότερα του ξεπλύματος βρώμικου χρήματος[83] και της ύπαρξης φορολογικών παραδείσων[84].

Αναφορικά με την ανταλλαγή φορολογικών δεδομένων μεταξύ των κρατών, οι δύο βασικοί άξονες συνίστανται στον αμερικάνικο νόμο Foreign Account Tax Compliance Act (FATCA) και στο Κοινό Πρότυπο Αναφοράς (Common Reporting Standard, CRS)[85] του ΟΟΣΑ. Ωστόσο, θα πρέπει να αναφερθεί ότι στο πλαίσιο των δύο διεθνών εργαλείων, δύνανται να ενυπάρχουν χρηματοοικονομικά και τραπεζικά δεδομένα, καθώς και άλλα προσωπικά δεδομένα. Παρά ταύτα, οι σκοποί της διαβίβασης είναι οι φορολογικοί και στο πλαίσιο αυτών γίνεται η διερεύνηση της ικανοποίησης των αρχών της νόμιμης επεξεργασίας των δεδομένων[86] και των μηχανισμών διαβίβασης.

Ως προς τον FATCA[87] (2010), θεσπίζει την απαίτηση να παρέχουν τα χρηματοπιστωτικά ιδρύματα των τρίτων χωρών πληροφορίες στις ΗΠΑ σε σχέση με τους λογαριασμούς ατόμων οι οποίοι φορολογούνται στις ΗΠΑ. Αυτή η

[83] Βλ. Δούβλης, Β. (2019). Η Υποχρεωτική Αυτόματη Ανταλλαγή Φορολογικών Πληροφοριών και η επέκτασή της στις Διασυνοριακές Ρυθμίσεις με την Οδηγία 2018/822/ΕΕ. *ΔΕΕ, 1,1-13.*

[84] Βλ. Cockfield, A. J. (2015). Bid Data and Tax Haven Secrecy. *Fla. Tax Rev., 18*, 483.

[85] Βλ. https://www.oecd.org/tax/automatic-exchange/common-reporting-standard/

[86]Βλ. Θεοχαροπούλου, Ε. (2021). *Η άμεση φορολογία της ψηφιακής οικονομίας και η δημιουργία αξίας*. Αφοί Κυριακίδη εκδόσεις Α.Ε., σελ. 37 κ. επ.

[87] Για τη Συμφωνία FATCA, Βλ. Θεοχαροπούλου, Ε. (2016). *Φορολογική διαφάνεια και Ανταλλαγή πληροφοριών σε καιρούς δημοσιονομικής και παγκόσμιας οικονομικής κρίσης*. Αφοί Κυριακίδη εκδόσεις Α.Ε., σελ. 293-313.

απαίτηση επιτυγχάνεται με την υπογραφή διμερών συμφωνιών με τις τρίτες χώρες[88] [89]. Στην Ελλάδα η Συμφωνία κυρώθηκε με τον Νόμο 4493/2017[90].

Παράλληλα, στο διεθνές πλαίσιο του ΟΟΣΑ για τη διασυνοριακή ανταλλαγή των φορολογικών δεδομένων (2014), τα συμμετέχοντα μέρη οφείλουν να υιοθετήσουν νομοθεσία η οποία να προβλέπει την αυτόματη συλλογή δεδομένων που αφορούν λογαριασμούς σε χρηματοπιστωτικά ιδρύματα ατόμων άλλης δικαιοδοσίας και τη μεταβίβαση αυτών των πληροφοριών στις αρμόδιες αρχές των κρατών που διατηρούνται οι λογαριασμοί, οι οποίες τα αποστέλλουν στις συμμετέχουσες χώρες.[91] Θα πρέπει να αναφερθεί ότι το πρότυπο του ΟΟΣΑ λαμβάνει υπόψη τον τόπο κατοικίας του φορολογούμενου, σε αντίθεση με τον FATCA, που εφαρμόζεται βάσει ιθαγένειας[92] [93]. Στο πλαίσιο εφαρμογής του προτύπου, θεσπίστηκε ο Ν. 4428/2016 (Κύρωση Πολυμερούς Συμφωνίας Αρμόδιων Αρχών για την Αυτόματη Ανταλλαγή Πληροφοριών Χρηματοοικονομικών Λογαριασμών) και ο Ν. 4490/2017 (Κύρωση της Πολυμερούς Συμφωνίας Αρμόδιων Αρχών για την Ανταλλαγή Εκθέσεων ανά Χώρα)[94].

Σε αμφότερες τις διεθνείς συμφωνίες, υπεύθυνη της επεξεργασίας των δεδομένων είναι η αρμόδια φορολογική αρχή της εκάστοτε χώρας. Για την Ελλάδα, ο υπεύθυνος της επεξεργασίας των δεδομένων είναι Ανεξάρτητη Αρχή Δημοσίων Εσόδων[95]. Ο GDPR προβλέπει στο άρθρο 23 παρ. 1 περ. ε τον περιορισμό μέσω νόμου της προστασίας των άρθρων 12 έως 22, του άρθρου 34, καθώς και του άρθρου 5, χάριν φορολογικών ζητημάτων. Στο πεδίο της προστασίας των φορολογικών δεδομένων τα οποία διαβιβάζονται σε τρίτες χώρες, η στάση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων κατευθύνει

[88] Θεοχαροπούλου, Ε. (2019). Οι νέες τεχνολογίες στο Φορολογικό Δίκαιο: Ευκαιρία ή απειλή; *ΔΙΜΕΕ, 3*, 300-308.

[89] Λωσταράκου, Κ. (2016). *Διακίνηση τραπεζικών δεδομένων και δικαιώματα υποκειμένων* σε Κοτσαλής Λ. (επιμ.) *Προσωπικά δεδομένα (Ανάλυση - Σχόλια - Εφαρμογή)*. Νομική Βιβλιοθήκη, σελ. 233.

[90] Θεοχαροπούλου, Ε. (2019). Οι νέες τεχνολογίες στο Φορολογικό Δίκαιο: Ευκαιρία ή απειλή; *ΔΙΜΕΕ, 3*, 300-308.

[91] Cockfield, A. J. (2019). Sharing Tax Information in the 21st Century: Big Data Flows and Taxpayers as Data Subjects. *Canadian Tax Journal*, *67*(4), 1179-1199.

[92] Δούβλης, Β. (2015). Διεθνείς δράσεις κατά της φοροδιαφυγής- φοροαποφυγής: «Η Μεγάλη Χίμαιρα»; *ΔΕΕ, 8-9, 769-787*.

[93] Βλ. Δούβλης, Β. (2019). Η Υποχρεωτική Αυτόματη Ανταλλαγή Φορολογικών Πληροφοριών και η επέκτασή της στις Διασυνοριακές Ρυθμίσεις με την Οδηγία 2018/822/ΕΕ. *ΔΕΕ, 1,1-13.*

[94] Θεοχαροπούλου, Ε. (2019). Οι νέες τεχνολογίες στο Φορολογικό Δίκαιο: Ευκαιρία ή απειλή; *ΔΙΜΕΕ, 3*, 300-308.

[95] Βλ. https://www.aade.gr/sites/default/files/2019-03/enimerwsi_potitwn_telik%CE%BF.pdf

τους υπεύθυνους της μεταφοράς αυτών των δεδομένων να στρέφονται στους μηχανισμούς διαβίβασης του άρθρου 46 και όχι του άρθρου 49 του GDPR[96] (οι μηχανισμοί των διασυνοριακών ροών αναλύονται στην ενότητα 8.5.2 της παρούσης). Αναλυτικότερα, ενώ η διαβίβαση των φορολογικών δεδομένων στοιχειοθετεί λόγο δημοσίου συμφέροντος (Αιτιολογική σκέψη 112 GDPR), ο οποίος ερείδεται και σε νόμο, ώστε να εφαρμοστεί ο μηχανισμός της παρέκκλισης του άρθρου 49 παρ. 1 περ. δ, εντούτοις οι επαναλαμβανόμενες διαβιβάσεις συμφωνιών συστηματικής ανταλλαγής πληροφοριών θα πρέπει να βασίζονται στον μηχανισμό των κατάλληλων εγγυήσεων του άρθρου 46. Στην ίδια κατεύθυνση, ειδικότερα για τις εξαγωγές δεδομένων στο πλαίσιο του FATCA, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων εστιάζει στους μηχανισμούς του άρθρου 46 παρ. 2 περ. α και του άρθρου 46 παρ. 3 περ. β του GDPR[97].

3.2.1 Φορολογικό απόρρητο

Ως απόρρητο λογίζεται κάθε γεγονός, πληροφορία ή στοιχείο, που ανεξαρτήτως κατόχου δεν είναι κοινοποιήσιμο σε τρίτους, εξυπηρετώντας μόνο τις ανάγκες του κατέχοντος[98]. Για το φορολογικό απόρρητο[99] έχει υποστηριχθεί ότι, εκτός από πλέγμα διασφάλισης της μυστικότητας των πληροφοριών και ως εκ τούτου της εμπιστοσύνης μεταξύ φορολογούμενου-αρχής[100], δύναται να αποτελεί και αιτία δυσχέρειας στην αποκάλυψη του παγκόσμιου φαινομένου των φορολογικών παραδείσων[101].

Ο GDPR αναφέρει ότι ακόμη και όταν δεν υπάρχει η συγκατάθεση του υποκειμένου, η εξυπηρέτηση του υπέρτερου έννομου συμφέροντος τρίτου ατόμου

[96] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_el

[97] European Data Protection Board. (2019). "Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA)." Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12-25-fatca_statement_en.pdf

[98] Δετσαρίδης, Χ. (2012). Φορολογικό απόρρητο και δημοσιοποίηση φορολογικών στοιχείων οφειλετών του Δημοσίου υπό το πρίσμα του εθνικού και ενωσιακού νομοθέτη. *Εφημερίδα Διοικητικού Δικαίου, 4,* 450-458.

[99] Βλ. Θεοχαροπούλου, Ε. (2016). *Φορολογική διαφάνεια και Ανταλλαγή πληροφοριών σε καιρούς δημοσιονομικής και παγκόσμιας οικονομικής κρίσης*. Αφοί Κυριακίδη εκδόσεις Α.Ε., σελ. 352 κ. επ.

[100] Φινοκαλιώτης, Κ. (2020). *Φορολογικό δίκαιο*. 6η έκδ. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 601.

[101] Cockfield, A. J. (2015). Bid Data and Tax Haven Secrecy. *Fla. Tax Rev., 18,* 483.

μπορεί να αποτελέσει νόμιμη βάση σύμφωνα με το άρθρο 6 παρ. 1 περ. στ. Ωστόσο, σύμφωνα με την ΑΠΔΠΧ[102], στην περίπτωση των φορολογικών δεδομένων εφαρμόζεται ως ειδικότερο το άρθρο 17 του Ν. 4174/2013, όπως συνέβαινε άλλωστε και με το προϊσχύον πλαίσιο του Κώδικα Φορολογίας Εισοδήματος και τον Ν. 2472/1997[103]. Πιο συγκεκριμένα, οι φορολογικές αρχές δεν μπορούν να διαβιβάσουν και να παρέχουν πρόσβαση σε τρίτους σε δεδομένα και σε περιπτώσεις τα οποία καλύπτονται από το φορολογικό απόρρητο. Θα πρέπει να αναφερθεί ότι το ζήτημα της απόφανσης για τα θέματα φορολογικού απορρήτου δεν αποτελεί αντικείμενο της αρμοδιότητας της ΑΠΔΠΧ[104]. Κάποιος τρίτος (εκτός του υποκειμένου των δεδομένων) μπορεί να έχει πρόσβαση σε φορολογικά δεδομένα που δεν καλύπτονται από το φορολογικό απόρρητο, όπως το ΑΦΜ (ΝΣΚ 552/1995, ΝΣΚ 39/1989), εφόσον έχει και υπέρτερο συμφέρον, πχ. Σε περίπτωση ασκηθείσας αγωγής.

3.2.1.1 Η ιδιωτικότητα του φορολογουμένου

Η αυξανόμενη επεξεργασία των φορολογικών δεδομένων, ιδιαίτερα των δεδομένων μεγάλης κλίμακας με τη χρήση των νέων τεχνολογιών, δύναται να επιφέρει επιπτώσεις στην ιδιωτικότητα. Αναλυτικότερα, στο πλαίσιο διεθνούς ανταλλαγής, η διασυνοριακή ροή των φορολογικών δεδομένων σε τρίτες χώρες αναδεικνύει ζητήματα σχετικά με το επίπεδο προστασίας της τρίτης χώρας και την πρόσβαση στα μεταβιβαζόμενα δεδομένα σε τρίτα μέρη. Παράλληλα, η αποκάλυψη φορολογικών πληροφοριών σχετιζόμενων με το εισόδημα μπορεί να προκαλέσει ζητήματα στη φυσική ασφάλεια του ατόμου, καθώς και να καλλιεργήσει κοινωνικές και πολιτικές διακρίσεις[105].

Αξίζει σε αυτό το σημείο να γίνει αναφορά σε δύο Γνωμοδοτήσεις της ΑΠΔΠΧ, οι οποίες έχουν ως αντικείμενο τη δημοσιοποίηση φορολογικών δεδομένων από το Υπουργείο Οικονομικών. Η ΑΠΔΠΧ στη Γνωμοδότηση 1/2011 σχετικά με το μέτρο της δημοσιοποίησης στοιχείων εισοδήματος φορολογουμένων από το Υπουργείο Οικονομικών, το οποίο θα στηριζόταν στην

[102]Βλ.https://www.dpa.gr/enimerwtiko/thematikes_enotites/dimosiostomeas/forologika/epexergsia_forologikwn_stoixeiwn

[103]Δετσαρίδης, Χ. (2012). Φορολογικό απόρρητο και δημοσιοποίηση φορολογικών στοιχείων οφειλετών του Δημοσίου υπό το πρίσμα του εθνικού και ενωσιακού νομοθέτη. *Εφημερίδα Διοικητικού Δικαίου, 4,* 450-458.

[104] Αρ. Απόφασης 52/2018

[105] Cockfield, A. J. (2019). Sharing Tax Information in the 21st Century: Big Data Flows and Taxpayers as Data Subjects. *Canadian Tax Journal*, *67*(4), 1179-1199.

παρ. 20 του άρθρου 8[106] του Ν. 3842/2010, εστιάζει στον κίνδυνο της χρήσης των δεδομένων αυτών για σκοπούς που επηρεάζουν άμεσα την ατομική ελευθερία συμμετοχής των ατόμων στην κοινωνική και οικονομική ζωή της χώρας, αλλά και στην έκθεση των προσώπων σε εγκληματικές ενέργειες (π.χ. εκβιασμούς)[107]. Η αρχή, επομένως, έκρινε ότι το μέτρο αυτό δεν συμβάδιζε με το δικαίωμα στην προστασία των δεδομένων. Αντίθετα, στην περίπτωση της δημοσιοποίησης των ληξιπρόθεσμων οφειλών προς το Δημόσιο, κατά το άρθρο 9[108] του Ν. 3943/2011, η ΑΠΔΠΧ έκρινε στη Γνωμοδότησή 4/2011 ότι η καταπολέμηση της φοροδιαφυγής δικαιολογεί τους περιορισμούς στο δικαίωμα στην προστασία των προσωπικών δεδομένων και το κρίνει ως πρόσφορο μέτρο, τονίζοντας και τη συνταγματική απαξία της μη εκπλήρωσης των φορολογικών υποχρεώσεων από μέρους των πολιτών[109].

3.3 Η διασυνοριακή ροή των χρηματοοικονομικών δεδομένων

Αναμφισβήτητα, ένα μεγάλο μέρος των οικονομικών δεδομένων παράγεται και διακινείται στο πλαίσιο λειτουργίας του χρηματοπιστωτικού τομέα. Ο χρηματοπιστωτικός τομέας συνίσταται από τα χρηματοπιστωτικά ιδρύματα, τις χρηματοοικονομικές υπηρεσίες, τις χρηματοπιστωτικές αγορές και τα χρηματοοικονομικά εργαλεία[110]. Στην παρούσα ενότητα θα αναλυθούν τα κύρια ζητήματα ιδιωτικότητας αφενός των μη νομισματικών χρηματοπιστωτικών

---

[106] «*Ο κατάλογος είναι διαθέσιμος στο διαδικτυακό τόπο της Γενικής Γραμματείας Πληροφοριακών Συστημάτων. Η πρόσβαση στον κατάλογο γίνεται κατόπιν ταυτοποίησης του χρήστη και περιορίζεται με βάση συγκεκριμένα ποσοτικά και ποιοτικά κριτήρια. Με απόφαση του Υπουργού Οικονομικών καθορίζονται όλες οι αναγκαίες λεπτομέρειες για την πρόσβαση στον κατάλογο αυτόν*.» Άρθρο 8 παρ. 20 του Ν. 3842/2010.

[107] Μήτρου, Λ. (2012). *Η δημοσιότητα της κύρωσης ή η κύρωση της δημοσιότητας*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 211 κ. επ.

[108] «*Τα στοιχεία των συνολικών ληξιπρόθεσμων οφειλών προς το Δημόσιο από κάθε αιτία και των ασφαλιστικών οφειλών προς τους Φορείς Κοινωνικής Ασφάλισης δημοσιοποιούνται υποχρεωτικά σε διαδικτυακό τόπο της Γενικής Γραμματείας Δημοσίων Εσόδων του Υπουργείου Οικονομικών, εφόσον η βασική ληξιπρόθεσμη οφειλή προς το Δημόσιο ή και τους Φορείς Κοινωνικής Ασφάλισης υπερβαίνει ανά φυσικό ή νομικό πρόσωπο ή νομική οντότητα το ποσό των εκατόν πενήντα χιλιάδων (150.000) ευρώ και η καταβολή της καθυστερεί για χρονικό διάστημα μεγαλύτερο του έτους…*» Άρθρο 9 παρ. 1 Ν. 3943/2011.

[109] Βλ. Αναστασόπουλος, Δ. (2016). *Φορολογικά δεδομένα και προστασία φορολογικού απορρήτου* σε *Ένωση Ελλήνων Νομικών e-ΘΕΜΙΣ, Επίκαιρα Ζητήματα Φορολογικού Δικαίου.* Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 285-301.

[110] Gurusamy, S. (2009). *Financial services and system*. Tata McGraw-Hill Education Private Limited, p. 3

ιδρυμάτων[111] (ασφαλιστικές εταιρείες, εταιρείες επενδύσεων χαρτοφυλακίου) και αφετέρου των νομισματικών χρηματοπιστωτικών ιδρυμάτων (τράπεζες).

3.3.1 Η διασύνδεση των δεδομένων στις χρηματιστηριακές αγορές

Απαραίτητα για τη λειτουργία των χρηματιστηριακών συναλλαγών και υπηρεσιών είναι τα προσωπικά δεδομένα. Ακόμη και με την εφαρμογή των μέτρων ασφαλείας της ψευδώνυμοποίησης και της ανωνυμοποίησης, η επιβολή της πολιτικής της γνώσης του πελάτη (know your costumer) στα χρηματιστήρια, η οποία στοχεύει στην αποτροπή του φαινομένου του ξεπλύματος βρώμικου χρήματος, επιβάλλει στον κλάδο αυτόν την επεξεργασία μεγάλης κλίμακας προσωπικών δεδομένων[112]. Όταν τα χρηματιστηριακά δεδομένα εξάγονται εκτός των συνόρων των χωρών, η επεξεργασία των δεδομένων πρέπει να συμμορφώνεται με τους μηχανισμούς της εκάστοτε χώρας για τη διαβίβαση των προσωπικών δεδομένων.

Οι οικονομικές οντότητες, που συμμετέχουν στις διεθνείς χρηματιστηριακές αγορές, εστιάζουν στην ασφάλεια των δεδομένων για την αντιμετώπιση του λειτουργικού χρηματοοικονομικού κινδύνου που κατά κύριο λόγο αφορά περιστατικά παραβίασης των προσωπικών δεδομένων. Πιο συγκεκριμένα, οι οικονομικές οντότητες θέτουν στο επίκεντρο του ενδιαφέροντος αφενός την αποτροπή επιβολής σε αυτές διοικητικών προστίμων και επιδίκασης αποζημιώσεων και αφετέρου τις αρνητικές επιπτώσεις στην αγορά (πτώση τζίρου, πτώση μετοχών). Οι ενδεχόμενες αρνητικές συνέπειες στη συνολικά διαμορφωμένη εταιρική φήμη, και ως αποτέλεσμα στην τιμή της μετοχής της εταιρείας που παραβιάστηκε, μπορούν να αποτελέσουν τροχοπέδη στην ενημέρωση της αρχής και των υποκειμένων των δεδομένων σχετικά με ένα τετελεσμένο περιστατικό παραβίασης των δεδομένων[113] [114].

[111] Νούλας, Α. Γ. (2005). *Χρήμα και τράπεζες*. Θεσσαλονίκη, σελ, 76 κ. επ.

[112] Polčák, R. (2017). Stock Exchange Interconnections and Legal Issues in Data Exchange. *Masaryk University Journal of Law and Technology*, *11*(2), 351-362.

[113] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2021). Σταθμίσεις συμφερόντων και νομοθετικές επιλογές στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). *ΔΙΤΕ, 3*, 367-376.

[114] Bianchi, D., & Tosun, O. K. (2018). *Cyber Attacks and Stock Market Activity. SSRN Electronic Journal.*

Στο ευρωπαϊκό θεσμικό επίπεδο των χρηματοπιστωτικών αγορών, έχει θεσπιστεί η Οδηγία 2014/65/ΕΕ[115] (MiFID II), η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 4514/2018 και αφορά τις αγορές χρηματοπιστωτικών μέσων[116]. Σε σχέση με την προστασία των προσωπικών δεδομένων, εγείρονται ζητήματα αφενός σε σχέση με την ιδιωτικότητα των πελατών στους οποίους παρέχονται επενδυτικές συμβουλές ή διαχείριση χαρτοφυλακίου και αφετέρου με την ιδιωτικότητα των ατόμων που εργάζονται στις επενδυτικές εταιρείες και παρέχουν επενδυτικές υπηρεσίες. Αναλυτικότερα, το άρθρο 25 παρ. 1 της Οδηγίας 2014/65/ΕΕ προβλέπει την αξιολόγηση των γνώσεων και των ικανοτήτων των εργαζομένων των επενδυτικών εταιρειών. Θα πρέπει να τονιστεί ότι, ενώ η νόμιμη βάση μπορεί να ερείδεται στην έννομη υποχρέωση των εταιρειών, η αυτοματοποιημένη λήψη αποφάσεων, σε σχέση με την αξιολόγηση, επιτρέπεται μόνο αν υφίσταται κάποια από τις εξαιρέσεις του άρθρου 22 παρ. 2 GDPR. Παράλληλα, το άρθρο 25 παρ. 2 της Οδηγίας προβλέπει την αξιολόγηση της χρηματοοικονομικής κατάστασης του πελάτη των επενδυτικών εταιρειών, προκειμένου να γίνεται γνωστό το εύρος του χρηματοοικονομικού κινδύνου που δύναται να αναλάβει. Η έννομη υποχρέωση των εταιρειών αποτελεί νόμιμη βάση επεξεργασίας[117], θα πρέπει, όμως, να εφαρμόζονται από τις επενδυτικές εταιρείες οι αρχές επεξεργασίας των δεδομένων και η διενέργεια εκτίμησης αντικτύπου της συστηματικής αξιολόγησης οικονομικών στοιχείων[118].

Υπό το πρίσμα των διασυνοριακών ροών των χρηματιστηριακών δεδομένων, θα πρέπει να αναφερθεί ότι υπάρχουν χώρες που εξαιρούν τα δεδομένα αυτά από το γενικό πρότυπο προστασίας των διεθνών διαβιβάσεων των δεδομένων τους. Ενδεικτικά, ο νόμος Personal Data Protection Act 25.326 της Αργεντινής εξαιρεί τα χρηματιστηριακά δεδομένα από την υποχρέωση της τρίτης χώρας να παρέχει επαρκές επίπεδο της προστασίας των προσωπικών δεδομένων. Ομοίως ορίζει και ο Law Nº 1581 της Κολομβίας. Γίνεται, λοιπόν, φανερό ότι η

---

[115] Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32014L0065

[116] Βλ. Πλιαβέσης, Γ. (2019). *Η προστασία των προσωπικών διδομένων στη σχέση τράπεζας – πελάτη.* Νομική Βιβλιοθήκη, σελ.139 κ. επ.

[117] Βλ. Πλιαβέσης, Γ. (2019). *Η προστασία των προσωπικών διδομένων στη σχέση τράπεζας – πελάτη.* Νομική Βιβλιοθήκη, σελ.139 κ. επ.

[118] Βλ. ΑΠΔΠΧ. Απόφαση Αριθ. 65/2018. (ΦΕΚ 1622/Β/10-5-2019). Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.

διασυνοριακή ροή των χρηματιστηριακών δεδομένων, όπως και των τραπεζικών, είναι και καταγράφεται από ορισμένες νομοθεσίες ως απαραίτητη, κάμπτοντας τους γενικούς περιορισμούς των διεθνών διαβιβάσεων σε τρίτες χώρες, οι οποίοι αποβλέπουν στη διαφύλαξη της ιδιωτικότητας των εξαγόμενων δεδομένων.

3.3.2 Η διασύνδεση των ασφαλιστικών δεδομένων

Όσον αφορά την ιδιωτική ασφάλιση, από το προσυμβατικό ακόμη στάδιο κατάρτισης της ασφαλιστικής σύμβασης, και μέχρι το στάδιο εκτίμησης του κινδύνου και καταβολής του ασφαλίσματος, τα προσωπικά δεδομένα των ασφαλιζόμενων υφίστανται επεξεργασία[119].

Εξάλλου, οι φορείς κοινωνικής ασφάλισης συλλέγουν από άλλες διοικητικές αρχές οικονομικά δεδομένα, όπως τα φορολογικά, με τα δηλωθέντα εισοδήματα να αποτελούν τη βάση υπολογισμού των οφειλόμενων εισφορών[120]. Ως μείζον ζήτημα αναδεικνύεται το εύρος των διαβιβαζόμενων δεδομένων, ενόψει της αρχής της ελαχιστοποίησης των δεδομένων.

Πιο συγκεκριμένα, η ΑΠΔΠΧ έχει κρίνει στην Απόφαση 1470/2000 ότι ορθώς ασφαλιστικό ταμείο μπορεί να συλλέγει φορολογικά δεδομένα (εκκαθαριστικό σημείωμα) για να διαπιστωθεί η ασφαλιστική κάλυψη της συζύγου, με την παροχή ενημέρωσης στο υποκείμενο για τα δεδομένα που επεξεργάζεται. Στη γνωμοδότησή της ΑΠΔΠΧ Αριθ. 1/2007 κρίθηκε βέβαια ότι η συλλογή της φορολογικής δήλωσης από ασφαλιστικό ταμείο για την υγειονομική περίθαλψη της συζύγου αντίκειται στην αρχή της αναλογικότητας, εφόσον μπορεί να χρησιμοποιηθεί άλλο πρόσφορο μέσο για τη διαπίστωση της κάλυψης των προϋποθέσεων της υγειονομικής περίθαλψης.

Παράλληλα, το ΔΕΕ έχει κρίνει[121] ότι το δίκαιο της Ένωσης αντιτίθεται στη διαβίβαση δεδομένων προσωπικού χαρακτήρα μεταξύ δύο διοικητικών αρχών και τη μεταγενέστερη επεξεργασία τους από αυτές χωρίς προηγούμενη ενημέρωση των υποκειμένων των δεδομένων.

---

[119] Χατζηνικολάου-Αγγελίδου, Ρ. (2014). *Ιδιωτικό Ασφαλιστικό Δίκαιο*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 125.

[120] Στεργίου, Α. (2017). *Δίκαιο κοινωνικής ασφάλισης*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 487.

[121] Απόφαση του ΔΕΕ της της 1ης Οκτωβρίου 2015 στην υπόθεση C-201/14 Smaranda Bara κ.λπ. κατά Președintele Casei Naționale de Asigurări de Sănătate κλπ.

Τόσο στον τομέα της ιδιωτικής όσο και της δημόσιας ασφάλισης δεν μπορούμε να παραβλέψουμε τον μεγάλο όγκο των δεδομένων που σχετίζονται με την υγεία των ατόμων[122], τα οποία αποτελούν ευαίσθητα προσωπικά δεδομένα (Άρθρο 9 παρ. 1 GDPR). Σε αυτό το πλαίσιο επεξεργασίας, θα πρέπει να διεξάγεται εκτίμηση του αντικτύπου της επεξεργασίας τέτοιων δεδομένων[123], αλλά και να λαμβάνονται όλα τα μέτρα που αφορούν την επεξεργασία ευαίσθητων προσωπικών δεδομένων.

Στον τομέα της ιδιωτικής ασφάλισης δύναται να ανταλλάσσονται προσωπικά δεδομένα στο πλαίσιο[124]: ανταλλαγής δεδομένων με νοσοκομεία, συνεργεία αυτοκινήτων, εταιρείες διαχείρισης αξιώσεων, υπηρεσίες εντοπισμού απάτης, δίκτυα πωλήσεων, όπως πρακτορεία και μεσίτες, εξωτερικά σημεία επαφών για την οδική βοήθεια ή τη νομική προστασία, ηλεκτρονικά καταστήματα για θέματα μάρκετινγκ. Σε σχέση με τη διασύνδεση των αρχείων των ασφαλιστικών εταιρειών, με σκοπό τη δημιουργία μιας ενοποιημένης βάσης πελατών, η ΑΠΔΠΧ έκρινε[125] ότι, εφόσον δεν περιέχονταν ευαίσθητα δεδομένα, δεν απαιτείται συγκατάθεση και ότι η συγκεκριμένη αυτή διασύνδεση δεν θα είχε ως αποτέλεσμα τη δημιουργία διακρίσεων σε βάρος των υποκειμένων των δεδομένων. Ως προς τα ευαίσθητα προσωπικά δεδομένα, τα οποία ενυπάρχουν κυρίως στις ασφάλειες υγείας και ζωής, η ΑΠΔΠΧ έκρινε[126] ότι τα ευαίσθητα προσωπικά δεδομένα μπορούν να διαβιβαστούν σε τρίτο (ασφαλιστική εταιρία) προκειμένου να υποστηριχθούν οι ισχυρισμοί του, στο πλαίσιο ένδικης υπόθεσης, αφού ο υπεύθυνος της επεξεργασίας (άλλη ασφαλιστική εταιρία) ενημερώσει το υποκείμενο των δεδομένων για τη διαβίβαση.

Ένα πολύ σημαντικό ζήτημα, στο οποίο και εστιάζει η Απόφαση 65/2018[127]της ΑΠΔΠΧ για τα ασφαλιστικά δεδομένα, είναι η αυτοματοποιημένη λήψη αποφάσεων που διενεργείται στον ασφαλιστικό κλάδο. Αναλυτικότερα, η αρχή θέτει στην πρώτη κατηγορία με τα είδη και τους σκοπούς επεξεργασίας, για

[122] Mulder, T., & Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, *28*(3), 261-274.

[123] Βλ. ΑΠΔΠΧ. Απόφαση Αριθ. 65/2018. (ΦΕΚ 1622/Β/10-5-2019). Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.

[124] Liapakis, X. (2018). A GDPR Implementation Guide for the Insurance Industry. *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, *7*(4), 34-44.

[125] Αρ. Απόφασης 81/2017

[126] Αρ. Απόφασης 56/2015

[127] Βλ. ΑΠΔΠΧ. Απόφαση Αριθ. 65/2018. (ΦΕΚ 1622/Β/10-5-2019). Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.

τα οποία απαιτείται διενέργεια εκτίμησης αντικτύπου, την αυτοματοποιημένη άρνηση της ασφαλιστικής παροχής. Αναδεικνύει, λοιπόν, το ζήτημα της προστασίας των ασφαλισμένων ατόμων ενόψει του ενδεχόμενου να απολέσουν την αποζημίωση από την ιδιωτική ασφάλιση, λόγω πλήρως αυτοματοποιημένων διαδικασιών στη διερεύνηση των συμβάντων, και ουσιαστικά θέτει ως απαιτούμενη διαδικασία την εκτίμηση αντικτύπου στις ασφαλιστικές εταιρίες που δρουν κατά αυτόν τον τρόπο.

3.3.3 Η διασυνοριακή ροή δεδομένων στο τραπεζικό σύστημα

Η διαβίβαση των προσωπικών δεδομένων πελατών των Τραπεζών μπορεί να γίνει είτε σε εταιρείες του ίδιου ομίλου εταιρειών, είτε σε τρίτες εταιρείες (πχ. εταιρείες διαχείρισης απαιτήσεων, εταιρείες που παρέχουν πληροφόρηση για την πιστοληπτική ικανότητα), είτε σε δημόσιες αρχές[128]. Ωστόσο, οι διαβιβάσεις αυτές δύνανται να γίνονται εντός του ορίου του ΕΟΧ, αλλά και εκτός αυτού. Οι διαβιβάσεις των δεδομένων σε τρίτες χώρες, στο πλαίσιο των μηχανισμών προστασίας των δεδομένων στον ΕΟΧ, περιλαμβάνουν ιδιαίτερα για τα χρηματοπιστωτικά ιδρύματα την αξιολόγηση του νομικού πλαισίου της τρίτης χώρας. Πιο συγκεκριμένα, ελλείψει απόφασης επάρκειας για την τρίτη χώρα από την Ευρωπαϊκή Επιτροπή, η εξεύρεση του μηχανισμού του άρθρου 46 GDPR που θα πρέπει να ακολουθηθεί, θα πρέπει να βασίζεται στα ειδικότερα χαρακτηριστικά των διαβιβαζόμενων δεδομένων από τις Τράπεζες, καθώς και τους νόμους που διέπουν τη λειτουργία τους στις τρίτες χώρες[129].

3.3.3.1 Η διαβίβαση των τραπεζικών δεδομένων

Οι διαβιβάσεις των προσωπικών δεδομένων από τις Τράπεζες στρέφονται κυρίως γύρω από τους άξονες της διαχείρισης του πιστωτικού κινδύνου και των ληξιπρόθεσμων απαιτήσεων. Είναι σκόπιμο στην παρούσα ενότητα να γίνει μία διαχρονική ανάλυση των ζητημάτων αυτών, με αφετηρία την πρόσφατη απόφαση

[128] Βλ. Πλιαβέσης, Γ. (2019). *Η προστασία των προσωπικών διδομένων στη σχέση Τράπεζας – πελάτη.* Νομική Βιβλιοθήκη, σελ.79 κ. επ.

[129] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

18/2019 της ΑΠΔΠΧ, η οποία έρχεται αντιμέτωπη και με τα δύο μεγάλα ζητήματα ιδιωτικότητας στο τραπεζικό σύστημα, εξετάζοντας το ζήτημα διεύρυνσης της λίστας των αποδεκτών της ΤΕΙΡΕΣΙΑΣ ΑΕ. Η απόφαση 18/2019 επιλαμβάνεται επί της αίτησης της ΤΕΙΡΕΣΙΑΣ ΑΕ για την αυτόνομη-άμεση πρόσβαση των Εταιρειών Διαχείρισης Απαιτήσεων, όταν ενεργούν για λογαριασμό των Εταιρειών Απόκτησης Απαιτήσεων στα αρχεία της ΤΕΙΡΕΣΙΑΣ ΑΕ (αρχεία ΣΑΥ[130] ή «μαύρη λίστα» και ΣΣΧ[131] ή «λευκή λίστα»).

Καταρχάς, όσον αφορά την ΤΕΙΡΕΣΙΑΣ ΑΕ[132], το τραπεζικό ελληνικό σύστημα προς εξυπηρέτηση της προστασίας της πίστης και της μείωσης των επισφαλειών ίδρυσε την ΤΕΙΡΕΣΙΑΣ το 1977, η οποία από το 1997 λειτουργεί ως ανώνυμη εταιρεία, με αντικείμενο την ανάπτυξη και τη διαχείριση ενός Αρχείου Δεδομένων Οικονομικής Συμπεριφοράς. Το αντικείμενο της λειτουργίας της σήμερα αφορά τη συγκέντρωση και τη διάθεση, σε συγκεκριμένους αποδέκτες[133], πληροφοριών οικονομικής συμπεριφοράς και δεδομένων συγκέντρωσης χορηγήσεων (για ιδιώτες και επιχειρήσεις), υποθηκών και προσημειώσεων μέσω πληροφοριακών συστημάτων[134] [135] [136] [137].

Τα δεδομένα οικονομικής συμπεριφοράς της ΤΕΙΡΕΣΙΑΣ ΑΕ διακρίνονται σε: «μαύρος» Τειρεσίας και «λευκός» Τειρεσίας. Ο «λευκός» Τειρεσίας περιλαμβάνει ενήμερες και σε καθυστέρηση οφειλές, όχι όμως βεβαιωμένες και απαιτητές[138]. Σε αντιδιαστολή, ο «μαύρος» Τειρεσίας, στα επιμέρους αρχεία «Σύστημα Αθέτησης Υποχρεώσεων» (ΣΑΥ) και «Σύστημα Υποθηκών – Προσημειώσεων» (ΣΥΠ), περιλαμβάνει βεβαιωμένες και απαιτητές οφειλές. Η επεξεργασία των δεδομένων του «λευκού» Τειρεσία, σε αντίθεση με

[130] Σύστημα Αθέτησης Υποχρεώσεων

[131] Σύστημα Συγκέντρωσης Χορηγήσεων

[132] Βλ. http://www.tiresias.gr

[133] Βλ. ΑΠΔΠΧ. Αρ. Απόφασης 18/2019

[134] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2004). Ηλεκτρονική επεξεργασία προσωπικών δεδομένων στο πεδίο της τραπεζικής δραστηριότητας (Νομικό Πλαίσιο). *Αρμενόπουλος 10, σελ*. 1377-1395.

[135] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2004). Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς από την «Τειρεσίας Α.Ε.» (θεσμικό πλαίσιο), *Δελτίο Ένωσης Ελληνικών Τραπεζών, Β΄ τριμ.,* σελ. 25-32.

[136] Βλ. Ιγγλεζάκης, Ι. (2006) *Προστασία προσωπικών δεδομένων στο σύστημα πληροφοριών ΤΕΙΡΕΣΙΑΣ.* Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

[137] Βλ. Μυλώση, Μ., Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2015). Προσωπικά δεδομένα οικονομικής συμπεριφοράς και η ηλεκτρονική επεξεργασία τους από την Τειρεσίας Α.Ε. *ΔΙΜΕΕ, 1*, σελ. 25-37.

[138] Βλ. ΑΠΔΠΧ. Αρ. Απόφασης 18/2019

τον «μαύρο» για τον οποίο η επεξεργασία στηρίζεται σε υπέρτερο έννομο συμφέρον, απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων[139] [140].

Ως αποδέκτες του αρχείου της ΤΕΙΡΕΣΙΑΣ ΑΕ ορίστηκαν αρχικά με αποφάσεις της ΑΠΔΠΧ: οι Τράπεζες, τα χρηματοπιστωτικά ιδρύματα και οι εταιρείες διαχείρισης πιστωτικών καρτών, καθώς και φορείς του δημοσίου τομέα, όχι τρίτοι μετέχοντες στις οικονομικές συναλλαγές και ακόμα λιγότερο μη μετέχοντες.[141] Εν συνεχεία, η ΑΠΔΠΧ διεύρυνε τους αποδέκτες με τις εταιρείες πρακτορείας επιχειρηματικών απαιτήσεων και τις εταιρίες χρηματοδοτικής μίσθωσης[142].

Πρόσφατα[143] η ΤΕΙΡΕΣΙΑΣ ΑΕ ζήτησε την έγκριση της ΑΠΔΠΧ για την ένταξη των Εταιρειών Διαχείρισης Απαιτήσεων (Ν. 4354/2015) στους νομιμοποιούμενους αποδέκτες των δεδομένων των αρχείων τόσο της «μαύρης λίστας» όσο και της «λευκής λίστας», με τους ίδιους όρους και προϋποθέσεις που ισχύουν για τις Τράπεζες. Η απάντηση της ΑΠΔΠΧ στο αίτημα διεύρυνσης των αποδεκτών της ΤΕΙΡΕΣΙΑΣ ΑΕ κινήθηκε κυρίως γύρω από την επισφαλή θέση των προσωπικών δεδομένων λόγω της σχέσης μεταξύ των Εταιρειών Διαχείρισης Απαιτήσεων και των Εταιρειών Απόκτησης Απαιτήσεων (οι οποίες κατέχουν την κυριότητα των απαιτήσεων) και την υποχρέωση διενέργειας εκτίμησης αντικτύπου.

Πιο συγκεκριμένα, η ΑΠΔΠΧ διατύπωσε την άποψη ότι το ζήτημα αυτό θα πρέπει να επιλυθεί με διάταξη νόμου, με τον ίδιο δηλαδή τρόπο που θεσπίζεται η λειτουργία και αρμοδιότητα των Εταιρειών Διαχείρισης Απαιτήσεων. Επιπλέον, η ΑΠΔΠΧ τονίζει την υποχρέωση λογοδοσίας των υπευθύνων της επεξεργασίας και προτείνει την επιβαλλόμενη[144] διενέργεια εκτίμησης αντικτύπου για να αξιολογηθεί μια τέτοια πρόσβαση σε μαζικά οικονομικά δεδομένα. Παράλληλα, τόνισε το καίριο ζήτημα της ανάλυσης των κινδύνων από τη διασύνδεση των Εταιρειών Διαχείρισης Απαιτήσεων με τις Εταιρείες Απόκτησης Απαιτήσεων, οι

[139] Βλ. ΑΠΔΠΧ. Αρ. Απόφασης 86/2002

[140] Βλ. Ν. 3869/2010 (Ρύθμιση των οφειλών υπερχρεωμένων φυσικών προσώπων και άλλες διατάξεις) άρθρο 4 παρ. 2 περ. γ. **(**ΦΕΚ Α΄130/3-8-2010).

[141] ΑΠΔΠΧ. Αρ. Απόφασης 109/31-03-1999, η οποία επαναλήφθηκε με την Αρ. Απόφασης 24/2004, (ΦΕΚ Β΄ 684/11-05-2004)

[142] ΑΠΔΠΧ. Αρ. Απόφασης 523/19-10-1999, η οποία επαναλήφθηκε με την Αρ. Απόφασης 25/2004, (ΦΕΚ Β΄ 684/11-05-2004)

[143] Βλ. ΑΠΔΠΧ. Αρ. Απόφασης 18/2019

[144] Βλ. ΑΠΔΠΧ. Απόφαση Αριθ. 65/2018. (ΦΕΚ 1622/Β/10-5-2019). Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.

οποίες δύνανται να είναι funds που εδρεύουν και εκτός ΕΕ. Η Αρχή υπογραμμίζει το ζήτημα της ανάλυσης των κινδύνων που μπορεί να έχει η εκτός ΕΕ διαβίβαση (*…πρέπει να αναλυθεί ο κίνδυνος διάθεσής τους σε ΕΑΑ, η οποία είναι δικαιούχος των υπό διαχείριση απαιτήσεων και η οποία δεν υπόκειται σε εποπτεία στην Ελλάδα, εφόσον μπορεί να βρίσκεται εγκατεστημένη οπουδήποτε στον κόσμο, οπότε θα πρέπει να αναλυθεί και ο κίνδυνος διαβίβασής τους εντός ή και εκτός ΕΕ.…*). Η ανάλυση των κινδύνων, όπως διατυπώθηκε, παραπέμπει στη διενέργεια εκτίμησης αντικτύπου της διασυνοριακής διαβίβασης σε τρίτη χώρα (Transfer Impact Assessment) η οποία έχει εισαχθεί ήδη ως επιταγή στα θεσμικά όργανα της ΕΕ[145].

Αυτή η εκτίμηση των κινδύνων της διασυνοριακής διαβίβασης, σύμφωνα με τις πρόσφατες συστάσεις[146] του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, θα πρέπει να εκκινεί με τις πιθανές διαβιβάσεις που μπορεί να διενεργηθούν σε τρίτες χώρες, βασιζόμενη εν προκειμένου στην έδρα των Εταιρειών Απόκτησης Απαιτήσεων. Επιπλέον, η αξιολόγηση αυτή θα πρέπει να περιλαμβάνει την εξακρίβωση του εργαλείου διαβίβασης, την αποτίμηση σχετικά με αυτό, αν δεν υφίσταται απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής, την εφαρμογή πρόσθετων μέτρων, αν κριθεί ότι είναι επιβεβλημένο από τις συνθήκες και τέλος την τακτική επανεκτίμηση του πλαισίου διαβίβασης από τον υπεύθυνο της επεξεργασίας.

Εν τέλει, σχετικά με την αποτίμηση της απόφασης 18/2019, θα πρέπει να τονιστεί η αρχή της λογοδοσίας που διαπνέει την απόφαση και ως εκ τούτου η υποχρέωση του υπεύθυνου της επεξεργασίας να αποδείξει τη συμμόρφωση, καθότι η ΑΠΔΠΧ δεν αποφάνθηκε για τη διεύρυνση των αποδεκτών και επέβαλε τη διενέργεια εκτίμησης αντικτύπου, η οποία θα πρέπει να εξετάσει και τον κίνδυνο διαβίβασης εκτός ΕΕ.

Ως προς το ζήτημα της διαβίβασης των δεδομένων της ΤΕΙΡΕΣΙΑΣ ΑΕ σε τρίτους (πχ. από τις Τράπεζες), θα πρέπει να διερευνηθεί αν υφίσταται η εκάστοτε

[145] European Data Protection Supervisor. (2020). Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en

[146] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

νόμιμη βάση επεξεργασίας υπό το άρθρο 6 του GDPR[147]. Στην 71/2001 απόφαση της ΑΠΔΠΧ, κρίθηκε ότι οι Τράπεζες πρέπει να διαβιβάζουν στις εταιρείες διαπίστωσης της πιστοληπτικής ικανότητας τα δεδομένα τα οποία οι ίδιες έχουν διαβιβάσει στην ΤΕΙΡΕΣΙΑΣ ΑΕ. Η διαβίβαση των δεδομένων οφειλετών από τις Τράπεζες στις Εταιρείες Ενημέρωσης Οφειλετών επιτρέπεται και χωρίς τη συγκατάθεση του οφειλέτη, με την προϋπόθεση ότι ο δανειστής έχει ενημερώσει με σαφήνεια τον οφειλέτη για τη διαβίβαση αυτή των δεδομένων του[148]. Για το ζήτημα της ενημέρωσης των οφειλετών, όταν τα δεδομένα τους διαβιβάζονται σε εταιρείες ενημέρωσης οφειλών οι οποίες δρουν ως εκτελούντες την επεξεργασία, η ΑΠΔΠΧ διατύπωσε στην Αρ. Απόφασης 98/2017 την υποχρέωση ειδικής ατομικής ενημέρωσης των οφειλετών. Βέβαια, θα πρέπει να σημειωθεί ότι η απόφαση 98/2017 εκδόθηκε με βάσει τον καταργηθέντα Ν. 2472/1997. Επί του παρόντος, και μετά την έναρξη εφαρμογής του GDPR, η ΑΠΔΠΧ δεν έχει κρίνει το ζήτημα του περιεχομένου και του τρόπου της ενημέρωσης των οφειλετών για τη διάθεση των προσωπικών τους δεδομένων σε Εταιρεία Ενημέρωσης Οφειλετών[149].

3.3.3.2 Τραπεζικό απόρρητο

Αρχικά, το τραπεζικό απόρρητο ως έννοια διακρίνεται σε γενικό και ειδικό τραπεζικό απόρρητο. Το γενικό τραπεζικό απόρρητο καλύπτει όλες τις τραπεζικές συναλλαγές και αναφέρεται στην υποχρέωση της Τράπεζας να τηρεί εχεμύθεια ως προς τις συναλλαγές των πελατών της. Το ειδικό τραπεζικό απόρρητο, από την άλλη, αποτελεί απόρρητο επί των τραπεζικών καταθέσεων όπως προβλέπεται στο ν.δ. 1059/1971.[150]

Εν γένει η έννοια του τραπεζικού απορρήτου μπορεί να αλληλεπικαλύπτεται με την προστασία της ιδιωτικότητας του ατόμου, υπό το πρίσμα της προστασίας ορισμένων οικονομικών προσωπικών δεδομένων. Ωστόσο, αφενός το νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων είναι ιδιαίτερα ευρύ για τις Τράπεζες ως υπεύθυνους της επεξεργασίας των δεδομένων και αφετέρου επιβάλλει υποχρεώσεις και δικαιώματα υπέρ όλων

[147] Βλ. Πλιαβέσης, Γ. (2019). *Η προστασία των προσωπικών διδομένων στη σχέση Τράπεζας – πελάτη.* Νομική Βιβλιοθήκη, σελ.124.

[148] Βλ. ΑΠΔΠΧ. Αρ. Απόφασης 87/2017

[149] Βλ. https://www.dpa.gr

[150] Βασιλάκη, Β. (2020). *Συντηρητική κατάσχεση στα χέρια τρίτου*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 198 κ. επ.

των υποκειμένων των δεδομένων και όχι μόνο των πελατών τους[151]. Υποστηρίζεται[152] ότι το πεδίο της σχέσης που μπορεί να έχει το τραπεζικό απόρρητο με τη νόμιμη επεξεργασία των δεδομένων δεν έχει αποκρυσταλλωθεί.

Όσον αφορά την άρση του τραπεζικού απορρήτου, το γενικό τραπεζικό απόρρητο κάμπτεται, αφού γίνει στάθμιση με τις προϋποθέσεις του άρθρου 6 GDPR, ενώ το ειδικό τραπεζικό απόρρητο κάμπτεται από προβλεπόμενη διάταξη νόμου[153]. Ενδεικτικά, κάμπτεται προς εξακρίβωση τελέσεως αξιόποινων πράξεων (όπως στον Ν. 4174/2013, Ν. 3691/2008, Ν. 1868/1989, και ν.δ. 1325/1972),[154] κυρίως για φορολογικούς σκοπούς[155], ενόψει του δικαιώματος κατάσχεσης των τραπεζικών καταθέσεων (Ν. 2915/2001), ενόψει του δικαιώματος κατάσχεσης των τραπεζικών καταθέσεων από το Δημόσιο (ν.δ. 356/1974, ΚΕΔΕ), αλλά και από τις περιπτώσεις που προβλέπει το τροποποιημένο ν.δ. 1059/1971.

3.4 Η διασυνοριακή ροή δεδομένων στο διεθνές εμπόριο

Αναμφισβήτητα, το διεθνές εμπόριο και ειδικότερα οι εξαγωγές και εισαγωγές προϊόντων και υπηρεσιών επηρεάζονται από τη διεθνή νομοθεσία για τη διασυνοριακή ροή των δεδομένων. Θα πρέπει να αναφερθεί ότι οι μηχανισμοί, οι οποίοι αναλύονται στο Β΄ μέρος του παρόντος πονήματος, και το εύρος των περιορισμών που θέτουν αλληλεπιδρούν με τις διεθνείς εξαγωγές. Ωστόσο, στην παρούσα ενότητα θα διερευνηθεί η σχέση των διεθνών εμπορικών συμφωνιών με την προστασία των προσωπικών δεδομένων και ειδικότερα της συμφωνίας GATS (General Agreement on Trade in Services) του Παγκόσμιου Οργανισμού Εμπορίου του 1994[156], η οποία διαδραματίζει κεντρικό ρόλο στα διεθνή ανακύπτοντα ζητήματα. Εξάλλου, θα πρέπει να σημειωθεί ότι η θέση σε ισχύ της Οδηγίας 95/46/ΕΚ έπεται κατά ένα μόλις έτος της Συμφωνίας GATS[157]. Αξίζει,

---

[151] Βλ. Πλιαβέσης, Γ. (2019). *Η προστασία των προσωπικών διδομένων στη σχέση Τράπεζας – πελάτη.* Νομική Βιβλιοθήκη, σελ. 101 κ. επ.

[152] Χριστοδούλου, Κ. (2020). *Δίκαιο Προσωπικών Δεδομένων*. Εκδ. Νομική Βιβλιοθήκη, σελ. 194.

[153] Βλ. Χρυσοχόου, Α. (2009). *Προστασία προσωπικών δεδομένων & τραπεζικό απόρρητο*, σελ. 48 κ. επ.

[154] Γνωμ. Εισ. ΑΠ 8/2018.

[155] Βλ. Φινοκαλιώτης, Κ. (2020). *Φορολογικό δίκαιο*. 6η έκδ. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 603 κ. επ.

[156] GATS, Annex 1B to the 1994 Marrakesh Agreement on Establishing the World Trade Organization (WTO Agreement).

[157] Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*(3), 201-221.

επιπλέον, να σημειωθεί ότι το οικονομικό αποτύπωμα των διασυνοριακών ροών των δεδομένων επηρεάζει το παγκόσμιο ΑΕΠ πλέον περισσότερο από το εμπόριο προϊόντων[158].

Πολλάκις έχει αναδειχθεί στη βιβλιογραφία το ζήτημα της αλληλεπίδρασης του διεθνούς εμπορικού δικαίου με τα μέτρα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων[159]. Στο πεδίο διερεύνησης της σχέσης των διασυνοριακών ροών των δεδομένων με το διεθνές εμπόριο πραγματοποιείται η στάθμιση των θετικών οικονομικών και κοινωνικών επιπτώσεων των διεθνών διαβιβάσεων με τους κινδύνους για την προστασία και την ασφάλεια των προσωπικών δεδομένων. Στην πράξη οι οικονομικές οντότητες και ειδικότερα οι ψηφιακές πλατφόρμες τάσσονται υπέρ των όσο το δυνατόν πιο ελεύθερων διεθνών διαβιβάσεων, ενώ από την άλλη πλευρά διαφαίνεται ότι ένα μέρος των αναπτυσσόμενων κρατών έχει υιοθετήσει περιορισμούς στις διεθνείς διαβιβάσεις[160], καθιστώντας σαφές ότι το ζήτημα αυτό δεν έχει μόνο οικονομικές πτυχές.

3.4.1 Οι περιορισμοί της διασυνοριακής ροής δεδομένων στο διεθνές εμπόριο

Στην παρούσα ενότητα επιχειρείται η προσπάθεια παρουσίασης των περιορισμών της διασυνοριακής ροής των δεδομένων, υπό το πρίσμα του διεθνούς εμπορίου. Σύμφωνα με μελέτη[161] του Ευρωπαϊκού Κέντρου Διεθνούς Πολιτικής Οικονομίας (European Centre for International Political Economy) οι περιορισμοί στις διεθνείς διαβιβάσεις, ως προς το διεθνές εμπόριο, διακρίνονται σε τέσσερις βασικές κατηγορίες με κριτήριο τον τρόπο εφαρμογής τους.

Αναλυτικότερα, οι τύποι των περιορισμών οι οποίοι επιφέρουν πρόσθετα κόστη στις οικονομικές οντότητες αποτελούνται από: την υποχρέωση τοπικής αποθήκευσης των δεδομένων (αντίγραφα των δεδομένων που παραμένουν εντός των συνόρων της χώρας), την υποχρέωση τοπικής επεξεργασίας των δεδομένων (αφορά την κύρια επεξεργασία των δεδομένων), καθολική απαγόρευση της διασυνοριακής ροής των δεδομένων, (αφορά συνήθως συγκεκριμένα είδη

[158] McKinsey Global Institute (2016). Digital Globalization: The New Era of Global Flow. Διαθέσιμο στο: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

[159] Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*(3), 201-221.

[160] UNCTAD (2019). Value Creation and Capture: Implications for Developing Countries. Digital Economy Report. Διαθέσιμο στο: https://unctad.org/webflyer/digital-economy-report-2019

[161] Ferracane, M. (2017). Restrictions on Cross-Border data flows: a taxonomy.

δεδομένων όπως τα ευαίσθητα) και το καθεστώς διασυνοριακής ροής υπό προϋποθέσεις. Αξίζει να αναφερθεί το παράδειγμα του Αυστραλιανού νόμου[162] ως προς την καθολική απαγόρευση διασυνοριακής ροής ηλεκτρονικών προσωπικών δεδομένων υγείας. Σε αυτό το πλαίσιο, θα μπορούσε ο GDPR να χαρακτηριστεί ως ένα καθεστώς διασυνοριακής ροής υπό όρους[163], όπως και η προϊσχύουσα Οδηγία 95/46/ΕΚ.

Η νομοθεσία της διασυνοριακής ροής δεδομένων σε κάθε χώρα είναι σε θέση να επηρεάσει τις διεθνείς εξαγωγές και εισαγωγές δεδομένων, αυξάνοντας το κόστος μίας εξαγωγής με την ανάγκη διερεύνησης του έτερου νομικού πλαισίου και συμμόρφωσης με αυτό. Ο χρόνος και το κόστος συμμόρφωσης με ένα θεσμικό πλαίσιο είναι πολύ σημαντικός στον τομέα της ανάπτυξης της επιχειρηματικής πρωτοβουλίας και των άμεσων ξένων επενδύσεων. Ο δείκτης *Doing Business*[164] της Παγκόσμιας Τράπεζας, ο οποίος κατατάσσει τις χώρες ανάλογα με το θεσμικό πλαίσιο που διέπει τις επιχειρήσεις τους, θα μπορούσε να περιλαμβάνει τους θεσμικούς περιορισμούς της διασυνοριακής ροής των δεδομένων στον παράγοντα του δείκτη με τίτλο: «Διασυνοριακές εμπορικές συναλλαγές»[165], στον οποίο επί του παρόντος αναφέρεται ότι δεν περιλαμβάνουν τον χρόνο και το κόστος συμμόρφωσης με το θεσμικό πλαίσιο της εκάστοτε οικονομίας.

3.4.1.1 Η Γενική Συμφωνία για το Εμπόριο Υπηρεσιών (General Agreement on Trade in Services, GATS) του Παγκόσμιου Οργανισμού Εμπορίου (ΠΟΕ)

Η νομοθεσία της εκάστοτε χώρας (μέλος του ΠΟΕ) για την προστασία των προσωπικών δεδομένων, και ειδικότερα το πλαίσιο που διέπει τις διασυνοριακές ροές δεδομένων σε όλο το φάσμα των ηλεκτρονικών υπηρεσιών, εγείρει εν δυνάμει ζητήματα σύγκρουσης με το άρθρο XVI της GATS[166]. Αναλυτικότερα, στην παρούσα ενότητα θα αναλυθεί το ζήτημα της ερμηνείας του XIV παρ. (c) περ. (ii), το οποίο αφορά τη θέσπιση νόμων για την προστασία των προσωπικών δεδομένων. Η συνεχώς αυξανόμενη τάση[167] των νομοθετικών περιορισμών στις διασυνοριακές ροές δεδομένων τα τελευταία έτη σε συνδυασμό με το γεγονός ότι

[162] Personally Controlled Electronic Health Record Act of 2012. Act No. 63, 2012. June 2012.

[163] Ferracane, M. (2017). Restrictions on Cross-Border data flows: a taxonomy.

[164] Βλ. https://www.doingbusiness.org/en/about-us

[165] Βλ. https://www.doingbusiness.org/en/methodology/trading-across-borders

[166] Weber, R. H. (2012). Regulatory autonomy and privacy standards under the GATS. *Asian J. WTO & Int'l Health L & Pol'y*, *7*, 25.

[167] Ferracane, M. (2017). Restrictions on Cross-Border data flows: a taxonomy

η διάταξη αυτή της GATS θεσπίστηκε το 1994 και δεν έχει κριθεί/αναλυθεί νομολογιακά από τον ΠΟΕ[168] αναδεικνύουν την ανάγκη αποσαφήνισής της.

Καταρχάς, το άρθρο XVI με τίτλο «Γενικές εξαιρέσεις» της GATS αναφέρει:

Υπό την προϋπόθεση ότι τα εν λόγω μέτρα δεν εφαρμόζονται κατά τρόπο ώστε να συνιστούν μέσο αυθαίρετης ή αδικαιολόγητης διάκρισης μεταξύ των χωρών όπου επικρατούν όροι, ή ένας συγκεκαλυμμένος περιορισμός στο εμπόριο υπηρεσιών, καμία από τις διατάξεις της συμφωνίας δεν μπορεί να θεωρηθεί ότι εμποδίζει την έγκριση ή την εφαρμογή από οποιοδήποτε μέλος της μέτρων:

……

(c) τα οποία είναι αναγκαία για την εξασφάλιση της συμμόρφωσης προς τους νόμους και τους κανονισμούς που δεν αντιβαίνουν στις διατάξεις της παρούσας συμφωνίας, συμπεριλαμβανομένων αυτών που αναφέρονται:

……

(ii) στην προστασία της ιδιωτικής ζωής των προσώπων, όσον αφορά την επεξεργασία και τη διάδοση δεδομένων προσωπικού χαρακτήρα, και την προστασία του εμπιστευτικού χαρακτήρα των ατομικών στοιχείων και λογαριασμών.

Από τις ανωτέρω διατάξεις καθίσταται σαφές ότι η νομοθεσία των κρατών για την προστασία των προσωπικών δεδομένων δύναται να αποτελεί εξαίρεση από την εφαρμογή της GATS, όταν η θέσπιση είναι αναγκαία (προϋποθέτει μία στάθμιση), δεν εφαρμόζεται αυθαίρετα ή προάγοντας αδικαιολόγητες διακρίσεις μεταξύ των χωρών και δεν θέτει συγκεκαλυμμένους περιορισμούς στο εμπόριο υπηρεσιών. Τα δικαιοδοτικά όργανα του ΠΟΕ έχουν υιοθετήσει[169], ως προς τις άλλες περιπτώσεις της παραγράφου (c), το τεστ αναγκαιότητας για τις συγκεκριμένες εξαιρέσεις, το οποίο μπορεί να αποτελέσει αναλογικό εργαλείο και για την περίπτωση της προστασίας των προσωπικών δεδομένων[170].

Συγκεκριμένα στην υπόθεση *US-Gambling* [171], διατυπώθηκε ότι για να καθίσταται ένα μέτρο αναγκαίο, θα πρέπει να μην υφίσταται στην προκειμένη

[168] Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*(3), 201-221.

[169] Mishra, N. (2020). Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?. *World Trade Review*, *19*(3), 341-364.

[170] Asinari, M. V. P. (2002). Is There any Room for Privacy and Data Protection within the WTO Rules?, *Elec. Comm'n L. Rev.*, *9*, 249.

[171] Βλ. https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm

περίπτωση άλλο μέτρο «εύλογα διαθέσιμο».[172] Το τεστ αναγκαιότητας, ακόμη, περιλαμβάνει τη στάθμιση και εξισορρόπηση του μέτρου με τον επιδιωκόμενο σκοπό[173]. Αναλυτικότερα, θα πρέπει να πραγματοποιείται μία αποτίμηση της συμβολής του νομοθετικού μέτρου με τον επιδιωκόμενο σκοπό, της σημαντικότητας των εννόμων συμφερόντων που προστατεύονται και του αντικτύπου της επίμαχης διάταξης ως προς τις εισαγωγές ή τις εξαγωγές[174]. Παρά ταύτα, θα πρέπει να αναφερθεί ότι από τις 44 υποθέσεις που έχουν κριθεί, σε μία μόνο διαπιστώθηκε ότι συντρέχει λόγος ύπαρξης εξαίρεσης από το πλαίσιο της GATS[175].

Όσον αφορά το ευρωπαϊκό πλαίσιο προστασίας των διασυνοριακών ροών δεδομένων, έχει υποστηριχθεί ότι ο μηχανισμός της αναγνώρισης της επάρκειας τρίτης χώρας από την Ευρωπαϊκή Επιτροπή, ο οποίος υφίσταται τόσο στην Οδηγία 95/46/ΕΚ όσο και στον GDPR, συγκρούεται με το άρθρο XIV της GATS.[176] Ειδικότερα, προβάλλεται η άποψη ότι η απόφαση επάρκειας δεν είναι ένα αναγκαίο μέτρο, εφόσον θα μπορούσαν να επιβληθούν ηπιότερα μέτρα, όπως μέτρα τα οποία να διαπνέονται από την αρχή της λογοδοσίας[177]. Επιπλέον, η επέκταση του πεδίου εφαρμογής του GDPR, σε σχέση με την Οδηγία 95/46/ΕΚ, και σε υπευθύνους ή εκτελούντες της επεξεργασίας που βρίσκονται και εκτός της

[172] WTO (2005). United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body. Διαθέσιμο στο: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(%40Symbol%3d+wt%2fds285%2f*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true

[173] WTO (2005). United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body. Διαθέσιμο στο: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(%40Symbol%3d+wt%2fds285%2f*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true

[174] WTO (2000). Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef- AB-2000-8-
Report of the Appellate Body. Διαθέσιμο στο: https://www.wto.org/english/tratop_e/dispu_e/161-169abr_e.pdf

[175] Κέντρο Ερευνών Δημοσίου Διεθνούς Δικαίου, & Ινστιτούτο Μικρών Επιχειρήσεων της Γενικής Συνομοσπονδίας Επαγγελματιών Βιοτεχνών Εμπόρων Ελλάδας (2016). Ο Παγκόσμιος Οργανισμός Εμπορίου, η GATS και η Ελληνική Αγορά Υπηρεσιών: μία συνοπτική παρουσίαση. Διαθέσιμο στο: https://www.athenspil.law.uoa.gr/fileadmin/depts/law.uoa.gr/athenspil/uploads/gats_memo_tlc.pdf

[176] Yakovleva, S., & Irion, K. (2016). The Best of Both Worlds-Free Trade in Services and EU Law on Privacy and Data Protection. *Eur. Data Prot. L. Rev., 2*, 191.

[177] Yakovleva, S., & Irion, K. (2016). The Best of Both Worlds-Free Trade in Services and EU Law on Privacy and Data Protection. *Eur. Data Prot. L. Rev., 2*, 191.

ΕΕ υπό προϋποθέσεις[178], θα μπορούσε να λεχθεί ότι αυστηροποιεί τα μέτρα προστασίας και δυσχεραίνει το πλαίσιο διερεύνησης της αναλογικότητάς τους. Ωστόσο, θα πρέπει να αναφέρουμε ότι οι αποφάσεις επάρκειας της Ευρωπαϊκής Επιτροπής δεν είναι ο μόνος διαθέσιμος μηχανισμός διασυνοριακής ροής των δεδομένων σε τρίτες χώρες, ώστε να επιφέρει αντικειμενικούς περιορισμούς στις εξαγωγές ή εισαγωγές κατά περίπτωση.

Παράλληλα, ως προς τον παράγοντα της σημαντικότητας του προστατευόμενου εννόμου συμφέροντος, εγείρονται ζητήματα για τον τρόπο αξιολόγησης αυτής. Πιο συγκεκριμένα, η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα στην ευρωπαϊκή έννομη τάξη αναδεικνύοντας την αναγκαιότητα της διαφύλαξής του, ενώ σε άλλες έννομες τάξεις, όπως των ΗΠΑ, δεν αποτελεί θεμελιώδες δικαίωμα. Επομένως, ως προς το ζήτημα της θέσπισης των ευρωπαϊκών περιορισμών για τη διασυνοριακή ροή των δεδομένων και ειδικότερα ως προς τον μηχανισμό επάρκειας της τρίτης χώρας, δύνανται να ανακύψουν ακόμη ζητήματα διαφορετικής αξιολόγησης του προστατευόμενου δικαιώματος[179].

Η μελέτη της διασυνοριακής ροής δεδομένων υπό το πρίσμα του διεθνούς εμπορίου αναδεικνύει την ανάγκη θέσπισης και λειτουργίας ενός παγκόσμιου συνεκτικού νομοθετικού πλαισίου.

[178] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα.

[179] Yakovleva, S. (2020). Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'. *The Journal of World Investment & Trade*, *21*(6), 881-919.

ΚΕΦΑΛΑΙΟ 4. ΤΑ ΟΙΚΟΝΟΜΙΚΑ ΔΕΔΟΜΕΝΑ ΩΣ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΤΑ ΠΑΓΚΟΣΜΙΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ 5ης ΚΑΙ 6ης ΓΕΝΙΑΣ: ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΔΙΑΚΙΝΗΣΗΣ ΜΕΣΩ ΑΥΤΩΝ

Η διασυνοριακή ροή των δεδομένων, μεταξύ των οποίων και των οικονομικών δεδομένων, πραγματοποιείται πλέον μέσω και των ασύρματων δικτύων 5ης γενιάς και αναμένεται και μέσω των δικτύων 6ης γενιάς. Καθώς ένα μεγάλο μέρος της παγκόσμιας διακίνησης των προσωπικών δεδομένων θα πραγματοποιείται μέσω των κυψελοειδών δικτύων, στο παρόν κεφάλαιο κρίθηκε αξιοσημείωτη η ανάλυσή τους υπό το πρίσμα του τομέα της προστασίας των προσωπικών δεδομένων, λόγω της εξελισσόμενης και αναμενόμενης επιρροής τους σε πολλούς τομείς δραστηριοτήτων των ατόμων.

4.1. Η αλληλεπίδραση του GDPR με την νέα γενιά δικτύων 5G και Διαδικτύου των Πραγμάτων[180]

(Δημοσιεύθηκε στο επιστημονικό περιοδικό IEEE ACCESS, doi:10.1109/ACCESS.2020.3000662)

4.1.1 Εισαγωγή

Στην παρούσα ενότητα, εξετάζεται το ειδικό πλαίσιο προστασίας των δεδομένων σε σχέση με τα δίκτυα 5G (5ης γενιάς), τα οποία αποτελούν την τρέχουσα εξέλιξη των τεσσάρων γενεών κυψελοειδών δικτύων[181]. Λαμβάνοντας υπόψη τα ανακύπτοντα πρακτικά ζητήματα τα οποία προκύπτουν από την τεχνολογία 5G, ο στόχος της παρούσας ενότητας είναι η παρουσίαση των αντίστοιχων νομικών λύσεων. Ο ψηφιακός αυτός μετασχηματισμός στις κινητές επικοινωνίες, που ξεκίνησε το 2020, θα επηρεάσει εφαρμογές ενός μεγάλου φάσματος υπηρεσιών στον τομέα της ενέργειας, στις υπηρεσίες μεταφορών, στον τραπεζικό τομέα, στον τομέα της υγείας, στα συστήματα βιομηχανικού ελέγχου[182] και σταδιακά την καθημερινή ζωή μέσω της χρήσης των έξυπνων συσκευών. Ως αποτέλεσμα, είναι καθοριστικής σημασίας η εξειδίκευση και η επισκόπηση της αλληλεπίδρασης του

[180] Η παρούσα ενότητα του κεφαλαίου δημοσιεύθηκε ως ερευνητική εργασία στην αγγλική γλώσσα στο επιστημονικό περιοδικό *IEEE ACCESS* υπό τον τίτλο:
Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR interference with next generation 5G and IoT networks. *IEEE Access*, *8*, 108052-108061.

Η ερευνητική εργασία υποστηρίχθηκε από το Ελληνικό Ίδρυμα Έρευνας και Καινοτομίας (ΕΛΙ.Δ.Ε.Κ.) στο πλαίσιο της Δράσης «Υποτροφίες ΕΛΙ.Δ.Ε.Κ. Υποψηφίων Διδακτόρων» (Αριθμός Υποτροφίας: 290)

[181] Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). What will 5G be?. *IEEE Journal on selected areas in communications*, *32*(6), 1065-1082.

[182] European Commission. (2019). "Commission Recommendation on Cybersecurity of 5G networks C 2335 final". Διαθέσιμο στο: https://eur-lex.europa.eu/eli/reco/2019/534/oj

ευρωπαϊκού νομικού πλαισίου προστασίας των προσωπικών δεδομένων με τα δίκτυα 5G, ως προς την αντιμετώπιση των ανακυπτόντων ζητημάτων ιδιωτικότητας.

Η ανάπτυξη των ψηφιακών εφαρμογών με συνέπεια την αύξηση των ψηφιακών δυνατοτήτων που παρέχονται σε άτομα και σε οντότητες, με κύριο στόχο την οικονομική πρόοδο, έχει αναδείξει την ανάγκη αφενός για ειδική προστασία και αφετέρου για αποσαφήνιση του υφιστάμενου πλαισίου προστασίας της ιδιωτικότητας. Πιο συγκεκριμένα, η προαναφερθείσα διερεύνηση του πλαισίου της προστασίας των προσωπικών δεδομένων είναι απαραίτητη κατά τη μαζική εφαρμογή της τεχνολογίας 5G, ώστε να επιτύχει τους στόχους της: την επικράτηση της στις τηλεπικοινωνίες και την υποστήριξη των ψηφιακών εφαρμογών. Συλλήβδην, η τεχνολογία 5G απαιτεί τη συνεργασία πολλών παρόχων δικτύων τόσο στο εσωτερικό όσο και στο εξωτερικό, υπό διαφορετικές δικαιοδοσίες. Η διασυνοριακή διάσταση της τεχνολογίας 5G εγείρει το ζήτημα της εναρμόνισης και συνεργασίας του ευρωπαϊκού[183] και διεθνούς δικαίου[184].

Επιπλέον, εκτός από την παγκόσμια επιρροή της τεχνολογίας 5G λόγω της τεχνικής της βάσης, η νομοθεσία της ΕΕ έχει διευρύνει τα όρια της εδαφικής προστασίας των προσωπικών δεδομένων στην ΕΕ. Αναλυτικότερα, εταιρείες και ιδιώτες[185] που βρίσκονται στην ΕΕ πρέπει να συμμορφώνονται με τον GDPR, αλλά και εκείνοι που βρίσκονται εκτός της ΕΕ, καθώς το επίκεντρο του ενδιαφέροντος έχει πλέον μεταφερθεί στην τοποθεσία των υποκειμένων των δεδομένων και της επεξεργασίας των δεδομένων ανθρώπων που ζουν εντός της ΕΕ[186].

Αναλυτικότερα, η παρουσίαση της αλληλεπίδρασης του ευρωπαϊκού νόμου περί προστασίας των δεδομένων με τις εφαρμογές του 5G αναλύεται παρακάτω, από το γενικό προς το ειδικό, επί τη βάσει των νομικών εργαλείων του GDPR, ο

[183] Ειδικότερα, ο GDPR ισχύει για τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ), ο οποίος περιλαμβάνει τις χώρες της ΕΕ και τη Νορβηγία, την Ισλανδία και το Λιχτενστάιν.

[184] Council of the European Union. (2019) "Note entitled: Law enforcement and judicial aspects related to 5G," Διαθέσιμο στο: http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf

[185] Karaduman, O. (2017). The general data protection regulation: Achieving compliance for EU and non-EU companies. *Bus. L. Int'l, 18,* 225.

[186] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Άρθρο 3, Αιτιολογική σκέψη 22. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

οποίος είναι ένας από τους αυστηρότερους και πιο ακριβείς νόμους για την προστασία των προσωπικών δεδομένων παγκοσμίως.

Τα προσωπικά δεδομένα συνίστανται σε οποιεσδήποτε πληροφορίες αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (άρθρο 4 παρ.1 του GDPR), συμπεριλαμβανομένης της διεύθυνσης IP και τα cookies. Η τεχνολογία 5G, η οποία θα εξαπλωθεί σε όλο το φάσμα του Διαδικτύου των Πραγμάτων (IoT)[187], πρόκειται να προσφέρει στο ασύρματο και ενσύρματο Διαδίκτυο ευρυζωνικές ταχύτητες της τάξης των 10 Gbps, περίπου εκατό φορές ταχύτερες από αυτές που ήταν θεωρητικά δυνατές με την προηγούμενη γενιά δικτύων[188]. Ως εκ τούτου, η διαβίβαση των μεγάλων δεδομένων θα αυξηθεί περισσότερο από ποτέ. Επομένως, αξίζει να αποσαφηνιστούν συγκεκριμένα ζητήματα που αφορούν την προστασία της ιδιωτικής ζωής, όπως είναι οι αρχές επεξεργασίας των δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων, οι υποχρεώσεις του υπευθύνου της επεξεργασίας, οι διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα, καθώς και οι μέθοδοι πρόληψης της ασφάλειας των δεδομένων από τον σχεδιασμό ενός πληροφοριακού συστήματος ή μιας μεθόδου επεξεργασίας.

4.1.2 Οι αρχές επεξεργασίας προσωπικών δεδομένων

Η απεικόνιση του πλαισίου προστασίας των δεδομένων που αφορά τα δίκτυα 5G, απαιτεί την παρουσίαση των επτά αρχών της επεξεργασίας των δεδομένων. Οι επτά βασικές αρχές, που παρουσιάζονται στο άρθρο 5 του GDPR, εκτός από τον καθορισμό των δικαιωμάτων του υποκειμένου των δεδομένων[189] και των υποχρεώσεων του υπεύθυνου[190] της επεξεργασίας δεδομένων (π.χ. εταιρεία) και

[187] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, vol. 54, no. 15, pp. 2787-2805.

[188] Blackman, C., Forge, S. (Scientific and Quality of Life Policies Directorate-General for Internal Policies Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies). (2019). "5G Deployment: State of play in Europe, USA and Asia". Διαθέσιμο στο : https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2019)631060

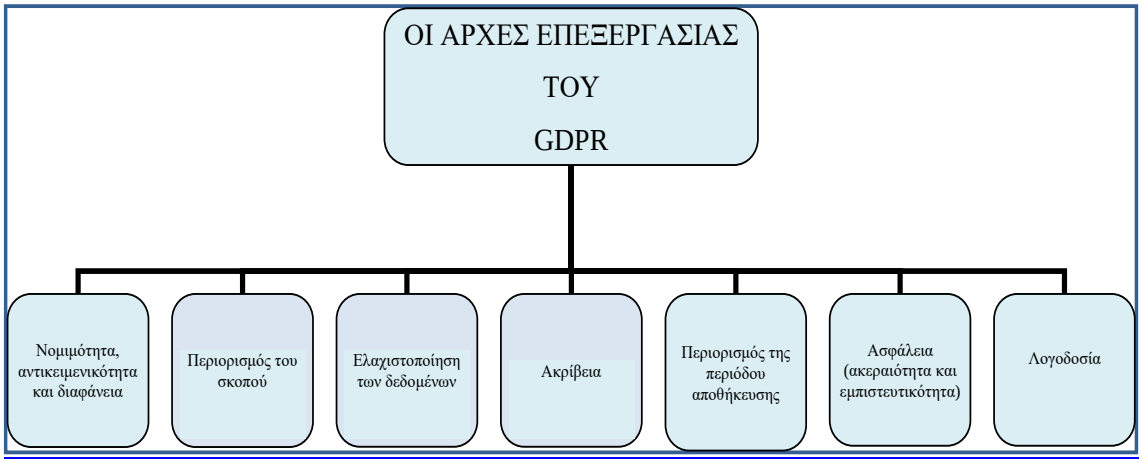
[189] «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο «υποκείμενο των δεδομένων». (Άρθρο 4 περ. 1 GDPR)

[190] «υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους. (Άρθρο 4 περ. 7 GDPR)

του εκτελούντα[191] της επεξεργασίας των δεδομένων, διέπουν και τις διασυνοριακές διαβιβάσεις δεδομένων.

Α. Οι επτά αρχές επεξεργασίες των δεδομένων

Το παρακάτω γράφημα απεικονίζει τις επτά αρχές επεξεργασίας των δεδομένων σύμφωνα με τον GDPR.



Εικόνα 2. Οι Αρχές επεξεργασίας του GDPR

1) ΝΟΜΙΜΟΤΗΤΑ, ΑΝΤΙΚΕΙΜΕΝΙΚΟΤΗΤΑ ΚΑΙ ΔΙΑΦΑΝΕΙΑ

Η νομιμότητα της επεξεργασίας εδράζεται στην αρχή της νομιμότητας, κατά την οποία, η επεξεργασία θα πρέπει να διαθέτει έναν πολύ συγκεκριμένο νόμιμο σκοπό επεξεργασίας[192], βάσει μιας συγκεκριμένης νόμιμης βάσης που θα πρέπει να έχει καθοριστεί. Η νόμιμη επεξεργασία απαιτεί τη συγκατάθεση[193] του υποκειμένου των δεδομένων ή την εξεύρεση κάποιας άλλης νόμιμης βάσης της επεξεργασίας. Αναλυτικότερα, εκτός από την συγκατάθεση, το άρθρο 6 παρ. 1 του GDPR περιλαμβάνει πέντε επιπλέον νόμιμες βάσεις επεξεργασίας (κατά την εκτέλεση μίας σύμβασης, κατά την άσκηση δημόσιας εξουσίας, κατά την συμμόρφωση με έννομη

[191] «εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας. (Άρθρο 4 περ. 8 GDPR)

[192] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* σελ. 69-72. Νομική Βιβλιοθήκη.

[193] «συγκατάθεση» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. (Άρθρο 4 περ. 11 GDPR)

υποχρέωση του υπευθύνου της επεξεργασίας για τους σκοπούς των εννόμων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτων[194], ή εάν απαιτείται ως προς τα ζωτικά συμφέροντα του υποκειμένου των δεδομένων)[195]. Όσον αφορά την αντικειμενικότητα και τη διαφάνεια, αυτές αναφέρονται στην απαίτηση οποιαδήποτε διαδικασία αφορά την επεξεργασία να μην διατηρείται κρυφή και να ενημερώνονται τα υποκείμενα των δεδομένων και οι δημόσιες αρχές, προκειμένου να είναι σε θέση να ασκήσουν τα δικαιώματά τους και να εξετάσουν τη συμμόρφωση με τον GDPR αντίστοιχα.

2) ΠΕΡΙΟΡΙΣΜΟΣ ΤΟΥ ΣΚΟΠΟΥ

Η αρχή του περιορισμού του σκοπού υπογραμμίζει ότι τα προσωπικά δεδομένα που συλλέγονται για έναν συγκεκριμένο σκοπό μπορούν να υποστούν περαιτέρω επεξεργασία μόνο για έναν σκοπό συμβατό με τον πρωταρχικό σκοπό συλλογής. Παράλληλα, αυτό σημαίνει ότι κάθε επόμενη επεξεργασία, εκτός από αυτές που έχουν αποδειχθεί συμβατές, πρέπει να βασίζεται σε μια άλλη νόμιμη βάση του άρθρου 6 του GDPR (πχ. μία νέα έγκυρη συγκατάθεση)[196].

3) ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Η ελαχιστοποίηση των δεδομένων μπορεί να θεωρηθεί μία έκφανση της αρχής της αναλογικότητας. Πιο συγκεκριμένα, η ελαχιστοποίηση αναφέρεται στο είδος και στον όγκο των προσωπικών δεδομένων, εισάγοντας το κριτήριο της αναγκαιότητας σε κάθε επεξεργασία. Επομένως, το κριτήριο της αναγκαιότητας δεν αναφέρεται μόνο στην ποσότητα των δεδομένων, αλλά και στην ποιότητά τους (πχ. ευαίσθητα δεδομένα, αντίκτυπος των δεδομένων)[197] [198].

---

[194] «τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα. (Άρθρο 4 περ. 10 GDPR)

[195] Council of Europe. (2018). *Handbook on European data protection law*. Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

[196] Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report*, *15*, 153.

[197] Kuner, C., Bygrave, L., Docksey, C., Svantesson, D., & de Terwagne, C. (2018). 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019).

4) ΑΚΡΙΒΕΙΑ

Η κατάσταση και η ποιότητα των προσωπικών δεδομένων προστατεύονται από την αρχή της ακρίβειας, η οποία επιβάλλει στον υπεύθυνο της επεξεργασίας την διατήρηση και επεξεργασία μόνο των ορθών προσωπικών δεδομένων, επιτάσσοντας την τροποποίηση ή διαγραφή των λανθασμένων στοιχείων ή μη ισχυόντων δεδομένων χωρίς καθυστέρηση.

5) ΠΕΡΙΟΡΙΣΜΟΣ ΤΗΣ ΠΕΡΙΟΔΟΥ ΑΠΟΘΗΚΕΥΣΗΣ

Ο περιορισμός της αποθήκευσης είναι η δεύτερη αρχή, η οποία πηγάζει από την αρχή της αναλογικότητας και αναφέρεται στην περιορισμένη διάρκεια της διατήρησης των προσωπικών δεδομένων[199]. Επομένως, η διατήρηση των προσωπικών δεδομένων γίνεται σε μία καθορισμένη χρονική περίοδο και στη συνέχεια πρέπει τα δεδομένα να διαγράφονται μετά την πάροδο της προβλεπόμενης επεξεργασίας τους[200]. Ο GDPR, ακόμη, ενθαρρύνει τον καθορισμό προθεσμιών της επεξεργασίας από τον υπεύθυνο επεξεργασίας (Αιτιολογική σκέψη 39).

6) ΑΣΦΑΛΕΙΑ (ΑΚΕΡΑΙΟΤΗΤΑ ΚΑΙ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ)

Η ασφάλεια των δεδομένων στοχεύει στη διασφάλιση της «ακεραιότητας» και της «διαθεσιμότητας». Τα δεδομένα πρέπει να είναι διαθέσιμα στα εξουσιοδοτημένα μέρη. Παράλληλα, δεν πρέπει να υπόκεινται σε αλλαγές ή να διαγράφονται από μη εξουσιοδοτημένα άτομα. Η τριπλέτα της «εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας» αποτελεί την απαίτηση της διασφάλισης των προσωπικών δεδομένων[201]. Παραδείγματα μέτρων που λαμβάνονται σε εναρμόνιση με τις απαιτήσεις ασφαλείας είναι: (α) η ψευδώνυμοποίηση (β) η ανωνυμοποίηση (γ) η δυνατότητα επαναφοράς των δεδομένων μετά από ένα περιστατικό που αντιβαίνει στις αρχές ασφάλειας και (δ)

---

[198] Για το ποιοτικό και ποσοτικό κριτήριο που εφαρμόζεται στο πλαίσιο της αρχής της αναλογικότητας, Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 73 κ. επ.

[199] Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. *Seton Hall L. Rev.*, *47*, 995.

[200] Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Case C-293/12, E.C.R. 238, 2014.

[201] Wolters, P. T. J. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility?. *International Data Privacy Law*, *7*(3), 165-178.

η δυνατότητα επαναπροσδιορισμού και συνεχούς επανεξέτασης όλων των μέτρων ασφαλείας που έχουν εφαρμοστεί[202].

7) ΛΟΓΟΔΟΣΙΑ

Η υποχρέωση των υπευθύνων επεξεργασίας να αποδεικνύουν ότι οποιαδήποτε επεξεργασία συμμορφώνεται με τους κανόνες για την προστασία των δεδομένων[203]. Είναι προφανές ότι η αρχή της λογοδοσίας είναι παράλληλα και μία επιπρόσθετη υποχρέωση των υπευθύνων της επεξεργασίας, εκτός από αυτές που περιγράφονται στο κεφάλαιο IV του GDPR.

4.1.3 Ασύρματα δίκτυα 5G και GDPR

Σε αυτήν την ενότητα του κεφαλαίου θα αναλυθούν τα καινοτόμα χαρακτηριστικά της τεχνολογίας 5G σε σχέση με τα χαρακτηριστικά της προηγούμενης γενιάς 4G, ενώ παράλληλα θα εξεταστεί η σχέση τους με υποχρεώσεις και δικαιώματα που απορρέουν από τον GDPR.

4.1.3.1 Τα καινοτόμα χαρακτηριστικά των δικτύων 5G και τα ζητήματα ιδιωτικότητας που εγείρουν

Οι καινοτομίες της τεχνολογίας 5G[204] που αποτελούν σημεία ενδιαφέροντος για την ιδιωτικότητα είναι οι εξής:

- Υψηλότερη ταχύτητα μετάδοσης δεδομένων (higher data rates): Τα δίκτυα 4G προσφέρουν ως ανώτατη ταχύτητα δεδομένων (μέγιστη εφικτή ταχύτητα για χρήση σε ιδανικές συνθήκες) τα 1Gbps και την ανώτατη ταχύτητα δεδομένων που συναντά ο χρήστης (εφικτή ταχύτητα για έναν χρήστη στο πραγματικό περιβάλλον του δικτύου) περίπου τα 10 Mbps. Στα δίκτυα 5G, η ανώτατη ταχύτητα δεδομένων αναμένεται να αυξηθεί έως και 20 Gbps και η ανώτατη ταχύτητα δεδομένων που συναντά ο

[202] Kuner, C., Bygrave, L., Docksey, C., Svantesson, D., & de Terwagne, C. (2018). 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019).

[203] Article 29 Working Party. (2010). "Opinion 1/2010 on the concepts of "controller" and "processor". Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

[204] Lemstra, W. (2018). Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implications. *Telecommunications Policy*, *42*(8), 587-611.

χρήστης θα βελτιωθεί 100 φορές σε σχέση με τα δίκτυα 4G και θα φτάνει έως και 1 Gbps[205].

- Υψηλότερη πυκνότητα του δικτύου (higher traffic density): ως αποτέλεσμα της τεχνολογίας massive MIMO (η massive MIMO είναι μια τεχνολογία που χρησιμοποιεί συστοιχίες κεραιών που περιέχουν μερικές εκατοντάδες κεραίες, ώστε να εξυπηρετούνται πολλές δεκάδες τερματικά χρηστών, συνδυάζοντας όλα τα οφέλη της τεχνολογίας MIMO αλλά σε μεγαλύτερη κλίμακα)[206] και της μετάδοσης σε χιλιοστομετρικά κύματα[207]. Πάρα ταύτα, το εξαιρετικά πυκνό κυψελοειδές δίκτυο 5G εξακολουθεί να είναι ένα δίκτυο περιορισμένης πυκνότητας[208].

- Υψηλότερη αξιοπιστία: η ικανότητα εγγύησης του ποσοστού επιτυχίας της μετάδοσης των δεδομένων σε καθορισμένες συνθήκες για μια συγκεκριμένη χρονική περίοδο στα 5G δίκτυα αναμένεται έως 99,999%[209].

- Χαμηλότερος λανθάνων χρόνος (lower latency): η τεχνολογία massive MIMO έχει επιφέρει μείωση στον λανθάνοντα χρόνο. Πιο συγκεκριμένα, τα δίκτυα 5G αναμένεται να μειώσουν τον λανθάνοντα χρόνο δέκα φορές σε επίπεδο χρήστη (έως 1 χιλιοστό του δευτερολέπτου) και στο μισό σε επίπεδο ελέγχου (έως 50 χιλιοστά του δευτερολέπτου), σε σύγκριση με τα δίκτυα 4G [210].

- Συνδεσιμότητα για περισσότερες συσκευές: Τα δίκτυα 5G υποστηρίζουν την πυκνότητα σύνδεσης έως 1 δισεκατομμυρίου συνδεδεμένων

[205] 3GPP, TR 22.891 v.2.0.0. "Feasibility Study on New Services and Markets Technology Enablers". Διαθέσιμο στο : https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897

[206] Ge, X., Tu, S., Mao, G., Wang, C. X., & Han, T. (2016). 5G ultra-dense cellular networks. *IEEE Wireless Communications*, *23*(1), 72-79.

[207] Kakalou, I., Psannis, K. E., Krawiec, P., & Badea, R. (2017). Cognitive radio network and network service chaining toward 5G: Challenges and requirements. *IEEE Communications Magazine*, *55*(11), 145-151.

[208] Ge, X., Tu, S., Mao, G., Wang, C. X., & Han, T. (2016). 5G ultra-dense cellular networks. *IEEE Wireless Communications*, *23*(1), 72-79.

[209] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (pp 34-307). New York: John Wiley & Sons.

[210] Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE access*, *3*, 1206-1232.

συσκευών ανά τετραγωνικό χιλιόμετρο (100 φορές περισσότερες συσκευές σε σύγκριση με δίκτυα 4G)[211].

- Χαμηλότερη κατανάλωση ενέργειας για την υποστήριξη του IoT: Τα δίκτυα 5G θα είναι 100 φορές πιο ενεργειακά αποδοτικά από τα δίκτυα 4G[212], με αποτέλεσμα την περαιτέρω ανάπτυξη του IoT.
- Παράλληλα, το γεγονός ότι η τεχνολογία 5G εξακολουθεί να βασίζεται σε IP[213], μπορεί να αποτελέσει έναν επιβαρυντικό παράγοντα για την προστασία της ιδιωτικότητας, καθώς ο εντοπισμός των διευθύνσεων IP μπορεί να οδηγήσει και σε αποκάλυψη περαιτέρω προσωπικών δεδομένων.

4.1.3.2 Δικαιώματα και υποχρεώσεις που απορρέουν από τον GDPR και σχετίζονται με τα δίκτυα 5G

Οι προστατευτικές διατάξεις που απορρέουν από τον GDPR διακρίνονται στα δικαιώματα των υποκειμένων των δεδομένων και τις υποχρεώσεις του υπεύθυνου και του εκτελούντα την επεξεργασία, με τον σεβασμό στα δικαιώματα να αποτελεί τμήμα των υποχρεώσεων.

4.1.3.2.1 Δικαιώματα του υποκειμένου των δεδομένων

ΔΙΚΑΙΩΜΑ ΕΝΗΜΕΡΩΣΗΣ (ΑΡΘΡΑ 13, 14): Είναι η κορωνίδα των δικαιωμάτων προστασίας δεδομένων, καθώς χωρίς την κατάλληλη ενημέρωση του υποκειμένου των δεδομένων δεν είναι δυνατή η άσκηση των άλλων δικαιωμάτων του. Η διατήρηση της διαφανούς επεξεργασίας των προσωπικών δεδομένων είναι καταλυτικής σημασίας στο πλαίσιο του δικαιώματος ενημέρωσης[214].

---

[211] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (pp 34-307). New York: John Wiley & Sons.

[212] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (pp 34-307). New York: John Wiley & Sons.

[213] Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications, 101,* 55-82.

[214] Article 29 Working Party. (2018). "Guidelines on transparency under Regulation 2016/679". WP260. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ (ΑΡΘΡΟ 15): Τα υποκείμενα των δεδομένων έχουν το δικαίωμα πρόσβασης στα προσωπικά δεδομένα τους και σε συγκεκριμένες πληροφορίες, οι οποίες θα πρέπει να παρέχονται από τον υπεύθυνο της επεξεργασίας σχετικά με αυτήν. Το δικαίωμα αυτό αποτελεί ένα αναπόσπαστο μέρος της ευρωπαϊκής νομοθεσίας για την προστασία των δεδομένων[215].

ΔΙΚΑΙΩΜΑ ΔΙΟΡΘΩΣΗΣ (ΑΡΘΡΟ 16): Το δικαίωμα αυτό έγκειται στη διατήρηση των προσωπικών δεδομένων στην ορθή μορφή, υπογραμμίζοντας κατ' ουσία την αρχή της ακρίβειας (αιτιολογική σκέψη 65 του GDPR).

ΔΙΚΑΙΩΜΑ ΣΤΗΝ ΔΙΑΓΡΑΦΗ/ΛΗΘΗ (ΑΡΘΡΟ 17): Το δικαίωμα του υποκειμένου να απαιτεί τη διαγραφή των προσωπικών δεδομένων του χωρίς αδικαιολόγητη καθυστέρηση. Το δικαίωμα στη λήθη καθιερώθηκε, πριν τη θέση σε ισχύ του GDPR, στην υπόθεση « *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González*» από το Ευρωπαϊκό Δικαστήριο[216].

ΔΙΚΑΙΩΜΑ ΠΕΡΙΟΡΙΣΜΟΥ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ (ΑΡΘΡΟ 18): Ένα ακόμη δικαίωμα στο πλαίσιο της πλήρους εποπτείας και ελέγχου των προσωπικών δεδομένων του υποκειμένου των δεδομένων είναι το δικαίωμα περιορισμού της επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν ισχύουν μία από τις τέσσερις προϋποθέσεις της παραγράφου 1.

ΔΙΚΑΙΩΜΑ ΓΝΩΣΤΟΠΟΙΗΣΗΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΔΙΑΓΡΑΦΗ, ΔΙΟΡΘΩΣΗ, ΠΕΡΙΟΡΙΣΜΟ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (ΑΡΘΡΟ 19): Το υποκείμενο των δεδομένων πρέπει να λαμβάνει γνώση για οποιαδήποτε διόρθωση ή διαγραφή προσωπικών του δεδομένων ή για τον περιορισμό της

[215] CJEU. YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S, 17 July 2014. Διαθέσιμο στο: https://curia.europa.eu/juris/liste.jsf?num=C-141/12&language=en

[216] CJEU. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 13 May 2014. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

επεξεργασίας, σε σχέση με οποιονδήποτε αποδέκτη, στον βαθμό που η γνωστοποίηση αυτή δεν είναι αδύνατη ή δυσανάλογη[217].

ΔΙΚΑΙΩΜΑ ΣΤΗ ΦΟΡΗΤΟΤΗΤΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ (ΑΡΘΡΟ 20): Αυτό το δικαίωμα αναφέρεται στη μετάδοση, κινητικότητα και στην ευελιξία των προσωπικών δεδομένων, παρέχοντας στα υποκείμενα των δεδομένων το δικαίωμα να λαμβάνουν τα προσωπικά δεδομένα τους σε ένα δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο[218], με την παράλληλη δυνατότητα διαβίβασης των δεδομένων αυτών σε άλλους υπευθύνους της επεξεργασίας.

ΔΙΚΑΙΩΜΑ ΕΝΑΝΤΙΩΣΗΣ (ΑΡΘΡΟ 21): Τα υποκείμενα των δεδομένων μπορούν να επικαλεσθούν το δικαίωμά τους να αντιταχθούν σε μία επεξεργασία προσωπικών δεδομένων[219]. Μια σημαντική έκφανση του δικαιώματος αυτού είναι η υποχρέωση του υπεύθυνου της επεξεργασίας να παρέχει τα μέσα στα υποκείμενα των δεδομένων για την υποβολή ηλεκτρονικών αιτημάτων και να ανταποκρίνεται στα αιτήματα άμεσα και ειδικότερα εντός ενός μήνα, με την παροχή εξηγήσεων σε περίπτωση μη συμμόρφωσης με τα υποβληθέντα αιτήματα (αιτιολογική σκέψη 59). Η διαφορά μεταξύ του δικαιώματος εναντίωσης με την ανάκληση της συγκατάθεσης έγκειται στη νόμιμη βάση της επεξεργασίας. Ειδικότερα, η ανάκληση της συγκατάθεσης απαιτεί την ύπαρξη της συγκατάθεσης ως νόμιμη βάση της επεξεργασίας, ενώ το δικαίωμα εναντίωσης μπορεί να αναφέρεται σε οποιαδήποτε νόμιμη βάση της επεξεργασίας.

ΔΙΚΑΙΩΜΑ ΝΑ ΜΗΝ ΥΠΟΚΕΙΤΑΙ ΣΕ ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΑΤΟΜΙΚΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΝ (ΑΡΘΡΟ 22): Συλλήβδην, η επεξεργασία που περιλαμβάνει αυτοματοποιημένη λήψη απόφασης, συμπεριλαμβανομένης της

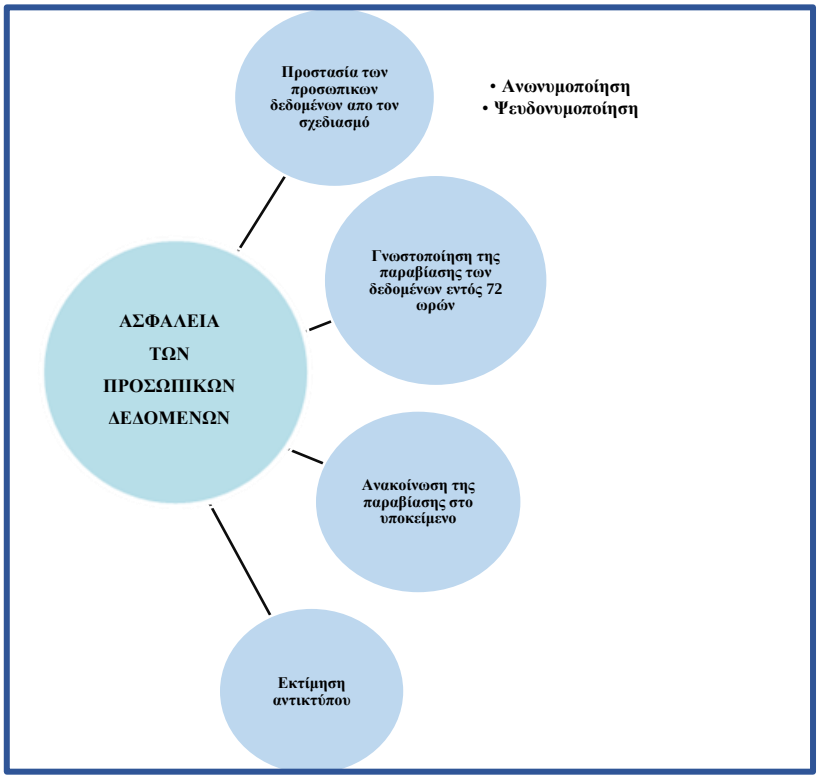
[217] Ad hoc Committee on Data Protection (CAHDATA). (2018). "Explanatory Report of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data". Strasbourg.

[218] Giurgiu, A., & Lallemang, T. (2017). The General Data Protection Regulation: a new opportunity and challenge for the banking sector. *Ace Magazine et Archives Online: Fiscalité, Comptabilité, Audit, Droit des Affaires au Luxembourg*, *1*, 3-15.

[219] Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report*, *15*, 153.

κατάρτισης προφίλ, απαγορεύεται από τον GDPR[220]. Επιτρέπεται σε περίπτωση εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης στην περίπτωση της συγκατάθεσης ή της ύπαρξης μίας σύμβασης, είτε σε περίπτωση υποστήριξης από το δίκαιο των κρατών-μελών ή το δίκαιο της ΕΕ[221].

4.1.3.2.2 Η υποχρέωση ασφάλειας των δεδομένων και οι εκφάνσεις της



Εικόνα 3.Μέτρα ασφαλείας του GDPR

Ο GDPR εξασφαλίζει την ασφάλεια των προσωπικών δεδομένων, θεσπίζοντας τα μέτρα της ψευδωνυμοποίησης και της ανωνυμοποίησης, τα οποία αποτελούν εκφάνσεις της προστασίας των δεδομένων από τον σχεδιασμό (privacy by design). Η τελευταία συμπληρώνει την αρχή της ελαχιστοποίησης δεδομένων και

[220] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[221] Kuner, C., Bygrave, L., Docksey, C., Svantesson, D., & de Terwagne, C. (2018). 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019).

αποτελεί μέτρο του εσωτερικού ελέγχου του επιπέδου ασφάλειας των προσωπικών δεδομένων.

Τα τέσσερα κριτήρια για την προστασία των προσωπικών δεδομένων από τον σχεδιασμό είναι τα εξής: (α) ελαχιστοποίηση των δεδομένων, (β) ελαχιστοποίηση της έκτασης της επεξεργασίας, (γ) ελαχιστοποίηση του χρόνου αποθήκευσης και (δ) ελαχιστοποίηση της προσβασιμότητας στα δεδομένα[222].

Επιπρόσθετα, ο GDPR θεσπίζει την ιδιαίτερα σημαντική υποχρέωση του υπευθύνου επεξεργασίας να ειδοποιεί την εποπτική αρχή για την παραβίαση προσωπικών δεδομένων εντός 72 ωρών ή να αιτιολογεί την περαιτέρω καθυστέρηση πάνω από αυτό το χρονικό όριο, ενώ το υποκείμενο των δεδομένων ή συνηθέστερα τα υποκείμενα των δεδομένων, πρέπει να λάβουν γνώση για μία παραβίαση δεδομένων με υψηλό κίνδυνο στα δικαιώματα των υποκειμένων των δεδομένων (αιτιολογική σκέψη 86)[223].

Η εκτίμηση του αντικτύπου σχετικά με την προστασία των δεδομένων (PIA) είναι μία προσέγγιση διαχείρισης κινδύνων, η οποία συμπληρώνει το πλαίσιο της προστασίας των δεδομένων από τον σχεδιασμό[224] [225], αξιολογώντας τον κίνδυνο κάθε επεξεργασίας. Η PIA πραγματοποιείται υποχρεωτικά στις εξής περιπτώσεις: (α) συστηματική και εκτεταμένη αξιολόγηση προσωπικών δεδομένων (δημιουργία προφίλ), (β) ύπαρξη μεγάλων και ευαίσθητων δεδομένων (άρθρο 9) ή (γ) ύπαρξη δεδομένων σχετικών με ποινικές καταδίκες και αδικήματα (άρθρο 10) και (δ) συστηματική παρακολούθηση μιας δημόσια προσβάσιμης περιοχής σε μεγάλη κλίμακα. Εάν το αποτέλεσμα της PIA καταδείξει υψηλό κίνδυνο, δημιουργείται η υποχρέωση του υπευθύνου επεξεργασίας να συμβουλεύεται την αρμόδια εποπτική αρχή πριν από κάθε επεξεργασία.

Επιπρόσθετα, μεγάλη σημασία πρέπει να αποδοθεί και στην υποχρέωση του υπεύθυνου της επεξεργασίας να σέβεται την ιδιωτικότητα σε σχέση με την τοποθεσία του υποκειμένου των δεδομένων, ιδιαίτερα λόγω της στήριξης των δικτύων σε IP.

---

[222] European Union Agency for Network and Information Security. (2019) "Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default," p 17.

[223] Karyda, M., & Mitrou, L. (2016). Data Breach Notification: Issues and Challenges for Security Management. In *MCIS* (p. 60).

[224] Commission Nationale de l'Informatique et des Libert´es (CNIL). (2018). "Privacy Impact Assessment: Methodology". February 2018 edition. Διαθέσιμο στο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

[225] Vemou, K., & Karyda, M. (2019). Evaluating privacy impact assessment methods: guidelines and best practice. *Information & Computer Security*.

4.1.3.3 Η συγκατάθεση του υποκειμένου των δεδομένων

Η συγκατάθεση του υποκειμένου ως νόμιμη βάση της επεξεργασίας είναι ένας από τους πιο συνήθεις τρόπους για να εκτελεστεί στην πράξη η επεξεργασία των προσωπικών δεδομένων, με την παράλληλη υποχρέωση του υπεύθυνου της επεξεργασίας να αποδείξει την παροχή της συγκατάθεσης.

Η ρητή συγκατάθεση είναι υποχρεωτική για την επεξεργασία ειδικών κατηγοριών δεδομένων, της διασυνοριακής μεταφοράς δεδομένων σε τρίτες χώρες και για την αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ[226].

Η ανάκληση της συγκατάθεσης είναι εξίσου σημαντική με τη συγκατάθεση, καθιστώντας αδύνατη κάθε μελλοντική επεξεργασία των προσωπικών δεδομένων, απαιτώντας τη διαγραφή αυτών των δεδομένων, εάν η επεξεργασία δεν βασίζεται σε άλλη νόμιμη βάση.

4.1.3.3.1 Η συγκατάθεση των παιδιών

Η διάταξη του άρθρου 8 διακρίνει τη συγκατάθεση των ανηλίκων σε δύο κατηγορίες με βάση την ηλικία τους: (α) 16 ετών και άνω, και (β) κάτω των 16 ετών. Στην πρώτη περίπτωση, η συγκατάθεση ενός ανηλίκου 16 ετών και άνω είναι επαρκής, ενώ στη δεύτερη περίπτωση είναι απαραίτητη η γονική συγκατάθεση ή η γονική έγκριση της συγκατάθεσης των ανηλίκων[227]. Ωστόσο, ο GDPR αναθέτει στις εθνικές νομοθεσίες, θυμίζοντας έτσι ευρωπαϊκή Οδηγία, να θεσπίσουν το κατάλληλο όριο ηλικίας για την υποχρεωτική γονική συγκατάθεση ή έγκριση, ορίζοντας ως γενικό όριο την ηλικία των 13 ετών.

4.1.4 Η συσχέτιση των δικτύων 5G με υποχρεώσεις και δικαιώματα που απορρέουν από τον GDPR

Η είσοδος της νέας τεχνολογίας 5G έχει επιφέρει τις επτά προαναφερθείσες καινοτομίες (βλ. υπό 4.1.3.1) σε σχέση με την απόδοση των δικτύων που δύνανται να εγείρουν ζητήματα στην προστασία των προσωπικών δεδομένων. Λόγω αυτών των τεχνικών χαρακτηριστικών, τα δίκτυα 5G αναμένεται να εξυπηρετούν ένα ευρύ φάσμα εφαρμογών αλλά και ολόκληρων τομέων του κοινωνικοοικονομικού γίγνεσθαι (όπως η ενέργεια, οι μεταφορές, οι τραπεζικές συναλλαγές, η υγεία, τα

[226]Article 29 Working Party. (2018). "Guidelines on transparency under Regulation 2016/679". WP260. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[227] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679. *ΔΙΜΕΕ, 1*, 5-19.

βιομηχανικά συστήματα ελέγχου, οι εκλογές)[228], με αποτέλεσμα την επεξεργασία τεράστιου όγκου δεδομένων[229]. Κατά συνέπεια, οι καινοτομίες των δικτύων 5G θα συμβάλλουν στην δυνατότητα των υποκειμένων των δεδομένων να δημιουργούν και να διαδίδουν περισσότερα προσωπικά δεδομένα στο Διαδίκτυο[230]. Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι οι σημαντικές διαφορές σε σύγκριση με τις προηγούμενες γενιές δικτύων αφορούν την φύση και την ένταση των πιθανών επιπτώσεων για την προστασία των προσωπικών δεδομένων, κυρίως λόγω της ευρύτερης εισβολής της τεχνολογίας 5G σε κοινωνικοοικονομικές λειτουργίες μέσω των επιδόσεων των χαρακτηριστικών που παρέχει[231].

Όσον αφορά την πρακτική εφαρμογή, ο ακόλουθος Πίνακας 1. παρουσιάζει τα σημαντικά νέα στοιχεία που συνοδεύουν την τεχνολογία 5G σε συσχέτιση με τα κύρια και με τα πρακτικής σημασίας δικαιώματα και υποχρεώσεις του GDPR, με βάση την ειδικότερη φύση και ένταση των επιπτώσεων των χαρακτηριστικών της τεχνολογίας 5G. Θα πρέπει να αναφερθεί ότι η ασύρματη τεχνολογία 5ης γενιάς δύναται να επηρεάσει υπό προϋποθέσεις κάθε υποχρέωση που απορρέει από τον GDPR. Επιπλέον, ο Πίνακας 1. αποτυπώνει τις υποχρεώσεις και τα δικαιώματα του GDPR που επηρεάζονται σε μεγαλύτερο βαθμό από την τεχνολογία 5G.

Πίνακας 1. Η συσχέτιση των χαρακτηριστικών των δικτύων 5G με υποχρεώσεις και δικαιώματα που απορρέουν από τον GDPR

	Υψηλή ταχύτητα μετάδοσης δεδομένων (High speed data rates)	Υψηλή πυκνότητα του δικτύου (High traffic density)	Συνδεσιμότητα περισσότερων συσκευών (IoT)	Εξάρτηση από IP
Δικαίωμα ενημέρωσης	X		X	
Δικαίωμα πρόσβασης			X	
Δικαίωμα διόρθωσης	X		X	
Δικαίωμα διαγραφής/λήθης	X		X	

[228] NIS Cooperation Group. (2019). "EU coordinated risk assessment of the cybersecurity of 5G networks". Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

[229] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G privacy: Scenarios and solutions. In *2018 IEEE 5G World Forum (5GWF)* (pp. 197-203). IEEE.

[230] Body of European Regulators for Electronic Communications. (2019). "Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem". Διαθέσιμο στο: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8910-report-on-the-impact-of-5g-on-regulation-and-the-role-of-regulation-in-enabling-the-5g-ecosystem

[231] NIS Cooperation Group. (2019). "EU coordinated risk assessment of the cybersecurity of 5G networks". Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

Δικαίωμα περιορισμού της επεξεργασίας	X		X	
Δικαίωμα γνωστοποίησης σχετικά με την διαγραφή, διόρθωση ή τον περιορισμό	X		X	
Δικαίωμα στη φορητότητα των δεδομένων			X	
Δικαίωμα εναντίωσης			X	
Δικαίωμα να μην υπόκειται σε αυτοματοποιημένη ατομική λήψη αποφάσεων	X	X	X	X
Συγκατάθεση του υποκειμένου και ανάκληση της συγκατάθεσης			X	
Συγκατάθεση των παιδιών			X	
Προστασία των προσωπικών δεδομένων από τον σχεδιασμό		X	X	X
Γνωστοποίηση της παραβίασης των δεδομένων εντός 72 ωρών	X		X	
Εκτίμηση αντικτύπου (PIA)	X	X	X	
Υποχρέωση σεβασμού της ιδιωτικότητας που σχετίζεται με την τοποθεσία του υποκειμένου		X		X

1) ΥΨΗΛΗ ΤΑΧΥΤΗΤΑ ΜΕΤΑΔΟΣΗΣ ΔΕΔΟΜΕΝΩΝ (HIGH SPEED DATA RATES):

Αυτή η αναβάθμιση που προσφέρει η τεχνολογία 5G, σε σχέση με την προηγούμενη γενιά, θα υποστηρίξει τους χρήστες του δικτύου με ταχύτητα μετάδοσης των δεδομένων αυξημένων Gbps, βελτιώνοντας τις εφαρμογές που κατασκευάζονται για τις κινητές συσκευές[232]. Ειδικότερα, οι νέες εφαρμογές που υποστηρίζουν τα δίκτυα 5G, όπως τα παιχνίδια σε πραγματικό χρόνο και πολλαπλών χρηστών (real time multi-user gaming), η εικονική/επαυξημένη πραγματικότητα (VR/ AR), τρισδιάστατη τηλεπαρουσία πολλαπλών τοποθεσιών (3D multi-site telepresence), υπερ-υψηλή ανάλυση σε βίντεο συνεχούς ροής (ultra –high resolution video streaming) και κοινή χρήση βίντεο-φωτογραφιών (photo-video sharing), απαιτούν την αύξηση των υφιστάμενων ταχυτήτων των δικτύων[233].

Επομένως, αξίζει να αναλυθεί ο τρόπος με τον οποίο η απόδοση των υψηλότερων ταχυτήτων, λόγω των νέων εφαρμογών και δυνατοτήτων μέσα στο περιβάλλον 5G δικτύου, επηρεάζει βασικές απαιτήσεις του GDPR. Επιπλέον, η υψηλή ταχύτητα δεδομένων οδηγεί σε παραγωγή τεράστιου όγκου δεδομένων[234]

[232] Goudos, S. K., Yioultsis, T. V., Boursianis, A. D., Psannis, K. E., & Siakavara, K. (2019). Application of new hybrid Jaya grey wolf optimizer to antenna design for 5G communications systems. *IEEE Access*, *7*, 71061-71071.

[233] Ahmadi, S. (2019). *5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards*. Academic Press.

[234] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018). 5G privacy: Scenarios and solutions. In 2018 IEEE 5G World Forum (5GWF) (pp. 197-203). IEEE.

και επομένως στην παραγωγή τεράστιου όγκου στις επεξεργασίες των δεδομένων που διενεργούνται. Οι κίνδυνοι για την προστασία της ιδιωτικότητας σε σχέση με τα δεδομένα μεγάλης κλίμακας (big data) αναφέρονται ως τα «τρία Vs»: (α) ο όγκος (volume) αναφέρεται στην ποσότητα των δεδομένων που υποβάλλονται σε επεξεργασία, (β) η ταχύτητα (velocity) αναφέρεται στην ταχύτητα των δεδομένων και (γ) η ποικιλία (variety) στον αριθμό και την ποικιλία του είδους των δεδομένων[235]. Παρόλο που η εκτίμηση του βαθμού στον οποίο ενδέχεται να επηρεαστούν τα προσωπικά δεδομένα δεν είναι δυνατή[236], είναι εφικτή η προσπάθεια εκτίμησης των επιπτώσεων της εκτεταμένης επεξεργασίας big data στα δίκτυα 5G σε σχέση με δικαιώματα και υποχρεώσεις που προβλέπει ο GDPR.

Οι υψηλότερες ταχύτητες δύνανται να συμβάλουν στην εκ των πραγμάτων αποτυχία ενημέρωσης του υποκειμένου των δεδομένων, σε σχέση με κάθε στοιχείο της επεξεργασίας δεδομένων τους, ως απόρροια της αδυναμίας εποπτείας όλων των επεξεργασιών των δεδομένων μέσω των δικτύων 5G σε μεγαλύτερο βαθμό απ' ό,τι στα δίκτυα 4G.

Επιπλέον, οι υψηλές ταχύτητες στις μεταδόσεις των δεδομένων μπορούν να επηρεάσουν τα δικαιώματα περιορισμού και διαγραφής των προσωπικών δεδομένων (δικαίωμα διόρθωσης, δικαίωμα διαγραφής/λήθης, δικαίωμα περιορισμού της επεξεργασίας, δικαίωμα γνωστοποίησης σχετικά με την διαγραφή, διόρθωση ή τον περιορισμό), κυρίως λόγω των ταχέων περαιτέρω διαβιβάσεων και διαμοιρασμού των δεδομένων.

Η εκτεταμένη διενεργούμενη επεξεργασία των δεδομένων, η οποία πραγματοποιείται χωρίς ανθρώπινη παρέμβαση, δημιουργεί έντονες ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής σε σχέση με τη δημιουργία προφίλ των υποκειμένων των δεδομένων.

Παράλληλα, η ταχύτερη διαβίβαση των προσωπικών δεδομένων δύναται να μειώσει τη δυνατότητα διασφάλισης της υποχρεωτικής κοινοποίησης μίας παραβίασης των δεδομένων η οποία στοχεύει στον περιορισμό της ζημίας. Λόγω των υψηλών ταχυτήτων ενδέχεται να μην γίνει άμεσα αντιληπτή η παραβίαση των δεδομένων, με αποτέλεσμα να παραβιαστεί το χρονικό όριο των 72 ωρών (άρθρο 33), με τις επιβαρυντικές συνέπειες για τον υπεύθυνο της επεξεργασίας. Επιπλέον, εφόσον η παραβίαση των δεδομένων θεωρείται ιδιαίτερα επιβλαβής για τα δικαιώματα των υποκειμένων, είναι υποχρεωτική και η κοινοποίηση του

[235] Council of Europe. (2018). *Handbook on European data protection law.* Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

[236] Council of Europe. (2018). *Handbook on European data protection law.* Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

γεγονότος της παραβίασης στα υποκείμενα εκτός από την εποπτική αρχή (άρθρο 34). Λαμβάνοντας υπόψη την ταχύτητα των μεταδιδόμενων δεδομένων, και ως εκ τούτου και ποιοτικά σημαντικών δεδομένων, η απαίτηση για την κοινοποίηση της παραβίασης στο υποκείμενο θα καταστεί μία πάγια τακτική συμμόρφωσης με το νομικό πλαίσιο σε περίπτωση παραβίασης δεδομένων.

Όσον αφορά τη διεξαγωγή της PIA, στο πλαίσιο αυτής της νέας τεχνολογίας, είναι υποχρεωτική λόγω υψηλών κινδύνων για την ιδιωτικότητα. Οι υψηλότερες ταχύτητες μπορούν να θεωρηθούν ένας καταλυτικός παράγοντας για τους κινδύνους, οι οποίοι ορίζονται στο άρθρο 35 του GDPR.

2) ΥΨΗΛΗ ΠΥΚΝΟΤΗΤΑ ΤΟΥ ΔΙΚΤΥΟΥ (HIGH TRAFFIC DENSITY):

Τα δίκτυα 5G θα είναι πυκνότερα και μεγαλύτερης δυναμικότητας από την προηγούμενη τεχνολογία 4G, χρησιμοποιώντας την τεχνολογία massive MIMO (βλ. παραπάνω υπό 4.1.3.1) [237]. Η υψηλή πυκνότητα των μικρών κελιών έχει ως αποτέλεσμα η άντληση των πληροφοριών του κελιού που σχετίζεται με ένα υποκείμενο δεδομένων να αποκαλύπτει τις πληροφορίες της τοποθεσίας του συγκεκριμένου υποκειμένου[238]. Η πυκνότητα δύναται να προκαλέσει αποκάλυψη πληροφοριών σχετικά με την τοποθεσία, επηρεάζοντας περαιτέρω υποχρεώσεις και δικαιώματα που απορρέουν από τον GDPR. Η παρακάτω ανάλυση επιχειρεί να καταδείξει τα νομικά ζητήματα που προκύπτουν και τα μέτρα που πρέπει να ληφθούν, προκειμένου να διατηρηθεί η προστασία δεδομένων στο πλαίσιο του εντοπισμού της τοποθεσίας των υποκειμένων μέσα στα πυκνά δίκτυα 5G.

Πιο συγκεκριμένα, ένα βασικό στοιχείο της τεχνολογίας 5G, που σχετίζεται με την πυκνότητα, είναι η υψηλή απόδοση στον εντοπισμό της συσκευής. Ο εντοπισμός και η εξαγωγή της ακριβούς τοποθεσίας του χρήστη της συσκευής, εκτός από την παροχή περισσότερων δυνατοτήτων για τις εφαρμογές εντοπισμού θέσης (location-based applications)[239], αναδεικνύει τα τρωτά σημεία της αποκάλυψης της θέσης του υποκειμένου, η οποία μπορεί με τη σειρά της να αποκαλύψει ή να επηρεάσει περαιτέρω προσωπικά δεδομένα, παρέχοντας

[237] Goudos, S. K., Deruyck, M., Plets, D., Martens, L., Psannis, K. E., Sarigiannidis, P., & Joseph, W. (2019). A novel design approach for 5G massive MIMO and NB-IoT green networks using a hybrid Jaya-differential evolution algorithm. *IEEE Access*, *7*, 105687-105700.

[238] Farhang, S., Hayel, Y., & Zhu, Q. (2015, September). PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks. In *2015 IEEE Conference on Communications and Network Security (CNS)* (pp. 263-271). IEEE.

[239] Koivisto, M., Hakkarainen, A., Costa, M., Kela, P., Leppanen, K., & Valkama, M. (2017). High-efficiency device positioning and location-aware communications in dense 5G networks. *IEEE Communications Magazine*, *55*(8), 188-195.

πληροφορίες που μπορούν να διασταυρωθούν σχετικά με μία τοποθεσία. Ως αποτέλεσμα, η πιθανή αποκάλυψη προσωπικών δεδομένων θα μπορούσε να χρησιμοποιηθεί για τη δημιουργία προφίλ και την παρακολούθηση των υποκειμένων.

Δεδομένου ότι είναι πιθανό να πραγματοποιηθεί αυτοματοποιημένη λήψη αποφάσεων μέσω της δημιουργίας προφίλ σε πυκνότερα δίκτυα, τα οποία θα μπορούν να ανιχνεύσουν την ακριβή τοποθεσία των υποκειμένων των δεδομένων, κρίνεται σημαντική η εξακρίβωση της ύπαρξης ή όχι της αυτοματοποιημένης λήψης αποφάσεων, ώστε να απατηθεί η διεξαγωγή της PIA πριν από κάθε επεξεργασία[240].

Επιπλέον, τα μέτρα με στόχο την προστασία των δεδομένων από τον σχεδιασμό, κατά τη διάρκεια του σχεδιασμού ή του επανασχεδιασμού των διαδικασιών ενός συστήματος πληροφορικής, θα πρέπει από τη θέση σε λειτουργία των δικτύων 5G να συνυπολογίζουν τον τρόπο με τον οποίο μία εφαρμογή ή συσκευή επεξεργάζεται τα προσωπικά δεδομένα του υποκειμένου (π.χ. δεδομένα τοποθεσίας, πρόσβαση σε αρχεία συσκευών ή εφαρμογών, ευαίσθητα προσωπικά δεδομένα). Παράλληλα, κάθε νέα δυνατότητα που παρέχει η τεχνολογία 5G θα πρέπει να αναλύεται μεμονωμένα και στην τεχνική της βάση, όσον αφορά ειδικά το προαναφερθέν κριτήριο (δ) (βλ. υπό 4.1.2) της προστασίας των προσωπικών δεδομένων από τον σχεδιασμό, το οποίο ορίζει την ελάχιστη διαθεσιμότητα των προσωπικών δεδομένων[241] και απορρέει επίσης από την αρχή της ελαχιστοποίησης δεδομένων.

3) ΣΥΝΔΕΣΙΜΟΤΗΤΑ ΠΕΡΙΣΣΟΤΕΡΩΝ ΣΥΣΚΕΥΩΝ (IOT):

Τα δίκτυα 5G αναμένεται να υποστηρίξουν κατά 100 φορές περισσότερες συσκευές σε σύγκριση με τα δίκτυα 4G[242]. Αναμφισβήτητα, η τεχνολογία 5G θα επηρεάσει τόσο τα υφιστάμενα όσο και τα επερχόμενα στοιχεία του IoT, στο οποίο

[240] Article 29 Working Party. (2018). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 250. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[241] European Union Agency For Network and Information Security. (2019). "Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default". (p. 17). Διαθέσιμο στο: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2

[242] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (p. 231). New York: John Wiley & Sons.

συναντάται, εκτός από επικοινωνία του χρήστη με την συσκευή, και πιο αποτελεσματική επικοινωνία από συσκευή σε συσκευή χωρίς ανθρώπινη συμμετοχή[243]. Τα νέα χαρακτηριστικά 5G, τα οποία προαναφέρθηκαν παραπάνω (βλ. υπό 4.1.3.1), όπως η χαμηλότερη καθυστέρηση, η χαμηλότερη κατανάλωση ενέργειας, η υψηλή αξιοπιστία και οι υψηλές ταχύτητες χρήστη, θα βελτιώσουν και θα επηρεάσουν το IoT [244]. Επιπλέον, η νέα τεχνολογία των κεραιών 5G στην αναδυόμενη τεχνολογία ασύρματης πρόσβασης Narrowband-IoT[245], αναμένεται να μειώσει τις απαιτήσεις για κατανάλωση ενέργειας κατά περίπου 10% [246].

Αναφορικά με τη δυνατότητα διασύνδεσης δύο συσκευών, η πρόσβαση σε μία συσκευή που είναι συνδεδεμένη σε άλλες μπορεί να θέσει σε κίνδυνο μέρος των συνδεδεμένων προσωπικών δεδομένων και των άλλων συσκευών[247]. Ο όγκος των δεδομένων και ο τρόπος επεξεργασίας τους θα μεταβληθεί με την είσοδο της τεχνολογίας 5G, λόγω του μεγαλύτερου αριθμού νέων συσκευών, της υψηλότερης συνδεσιμότητας μεταξύ των συσκευών, και ως εκ τούτου της ύπαρξης big data.

Σε αυτό το πλαίσιο, η άσκηση των δικαιωμάτων των υποκειμένων μπορεί να καταστεί από ιδιαίτερα περίπλοκη μέχρι και ανέφικτη. Πιο συγκεκριμένα, στο περιβάλλον του IoT, είναι συχνά ασαφές το ποιός έχει το δικαίωμα της πρόσβασης και της συλλογής δεδομένων μέσω διαφορετικών συσκευών[248], και γενικά οποιασδήποτε μορφής επεξεργασίας. Επιπλέον, δημιουργείται για τα υποκείμενα των δεδομένων ένα ασαφές πλαίσιο άσκησης των δικαιωμάτων τους[249] (το

---

[243] Hošek, J. (2016). *Enabling Technologies and User Perception Within Integrated 5G-IoT Ecosystem*. Vysoké učení technické v Brně, nakladatelství VUTIUM.

[244] Ni, J., Lin, X., & Shen, X. S. (2018). Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE Journal on Selected Areas in Communications*, *36*(3), 644-657.

[245] Η τεχνολογία NB-IoT είναι βασισμένη στο κυψελοειδές IoT και υποστηρίζει μεγάλη συνδεσιμότητα συσκευών, κάλυψη ευρείας περιοχής, εξαιρετικά χαμηλή κατανάλωση ενέργειας και εξαιρετικά χαμηλό κόστος. Βλ. Chen, X., Li, Z., Chen, Y., & Wang, X. (2019). Performance analysis and uplink scheduling for QoS-aware NB-IoT networks in mobile computing. *IEEE Access*, *7*, 44404-44415.

[246] Goudos, S. K., Deruyck, M., Plets, D., Martens, L., Psannis, K. E., Sarigiannidis, P., & Joseph, W. (2019). A novel design approach for 5G massive MIMO and NB-IoT green networks using a hybrid Jaya-differential evolution algorithm. *IEEE Access*, *7*, 105687-105700.

[247] Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018, July). 5G privacy: Scenarios and solutions. In *2018 IEEE 5G World Forum (5GWF)* (pp. 197-203). IEEE.

[248] Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report*, *15*, 153.

[249] Loideain, N. N. (2019). A port in the data-sharing storm: the GDPR and the Internet of things. *Journal of Cyber Policy*, *4*(2), 178-196.

δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης, το δικαίωμα στη διαγραφή/λήθη, το δικαίωμα περιορισμού της επεξεργασίας, το δικαίωμα γνωστοποίησης σχετικά με την διαγραφή, διόρθωση ή τον περιορισμό, το δικαίωμα στη φορητότητα των δεδομένων, το δικαίωμα εναντίωσης), λόγω του γεγονότος ότι δεν γνωρίζουν το περιεχόμενο των επεξεργαζόμενων δεδομένων τους, το είδος της επεξεργασίας, τον υπεύθυνο της επεξεργασίας των δεδομένων και τον εκτελούντα την επεξεργασία των δεδομένων. Είναι σημαντικό να τονιστεί η σημασία της υποχρέωσης για τον υπεύθυνο της επεξεργασίας να ενημερώνει τα υποκείμενα σχετικά με τον ακριβή τρόπο με τον οποίο τα δεδομένα τους θα χρησιμοποιηθούν, ιδιαίτερα σε ένα τόσο σύνθετο πλαίσιο επεξεργασίας.

Επιπρόσθετα, η ανάκληση της συγκατάθεσης του υποκειμένου θα πρέπει να είναι εξίσου εύκολη με τη συγκατάθεση για τα υποκείμενα. Αυτή η απαίτηση καθίσταται αφενός δύσκολη και αφετέρου επιβεβλημένη σε μία πλατφόρμα διαμοιρασμού.

Όσον αφορά τη συγκατάθεση των ανηλίκων, στο IoT είναι καίριας σημασίας τόσο για την προστασία των προσωπικών δεδομένων όσο και για την ασφάλεια των παιδιών στο περιβάλλον του κυβερνοχώρου. Το ζήτημα που αναδεικνύεται είναι η διασφάλιση στην πράξη της γονικής συγκατάθεσης (για ανηλίκους κάτω των 16 ετών, ή και λιγότερο με κατώτατο όριο τα 13 έτη), όταν πολλά μέλη της οικογένειας κατέχουν και διαχειρίζονται μέσα από διαφορετικούς λογαριασμούς (ακόμη και αν έχει επιβεβαιωθεί η χρήση από ενήλικα) έξυπνες συσκευές. Εκτός από το ζήτημα της έγκυρης συγκατάθεσης, είναι υπό αμφισβήτηση, ακόμη, η έκταση και ο σκοπός της χορηγηθείσας συγκατάθεσης, όταν γίνεται επεξεργασία απεριόριστων δεδομένων, όπως στην περίπτωση των παιχνιδιών στο περιβάλλον του IoT και γενικά των συσκευών που έχουν σχεδιαστεί για τον σκοπό της καταγραφής και αποθήκευσης αρχείων με συνομιλίες παιδιών[250]. Ως προς τα ζητήματα γονικού ελέγχου, για τα οποία έχει γίνει προσπάθεια αντιμετώπισης από τα προηγούμενα δίκτυα 4G[251], θα πρέπει να τονιστεί ότι η διασφάλιση της γονικής συγκατάθεσης προϋποθέτει τον προηγούμενο γονικό έλεγχο. Η γονική συγκατάθεση ακολούθως θα πρέπει να παρέχεται μετά την παροχή των απαραίτητων πληροφοριών για κάθε επεξεργασία δεδομένων και την

[250] Council, N. C. (2016). Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys. *Oslo, NCC*.

[251] 3GPP, 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)." Διαθέσιμο στο: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=641

επαλήθευση της ηλικίας, αλλά και της κατοχής της επιμέλειας των ανηλίκων, με την ευθύνη του υπευθύνου της επεξεργασίας των δεδομένων.

Ως προς τη νόμιμη βάση της συγκατάθεσης για μία επεξεργασία, τα πολλαπλά δεδομένα και οι επεξεργασίες μέσα στο IoT δύνανται να βάλλουν ενάντια στην απαίτηση του GDPR για σαφή συγκατάθεση, η οποία συνοδεύεται από αντίστοιχη ενημέρωση[252] και αντιστοιχεί σε μία συγκεκριμένη επεξεργασία δεδομένων.

Όσον αφορά την αυτοματοποιημένη λήψη αποφάσεων, η διασφάλιση της κατάλληλης πληροφόρησης για τους χρήστες του IoT είναι καίριας σημασίας, προκειμένου να κατανοήσουν τις συνέπειες αυτής της επεξεργασίας για εκείνους[253], καθώς ανάμεσα σε διαφορετικές συσκευές καθίσταται ευκολότερη η άντληση μεγαλύτερου αριθμού πληροφοριών, ως προς τις διαφορετικές πτυχές της προσωπικότητας, της συμπεριφοράς, των ενδιαφερόντων και των συνηθειών ενός ατόμου οι οποίες μπορούν να αναλυθούν και να αξιολογηθούν[254].

Όσον αφορά την κοινοποίηση των παραβιάσεων των δεδομένων και ιδιαίτερα την αναφορά της παραβίασης δεδομένων, η εστίαση θα πρέπει να γίνει στο ζήτημα της απαίτησης καταγραφής κάθε μεμονωμένης παραβίασης δεδομένων. Ιδιαίτερα ως προς το IoT, είναι δυνατόν να συντελεστούν πολλαπλές παραβιάσεις δεδομένων από μία μόνο αιτία μέσω διαφορετικών συσκευών και με διαφορετικό περιεχόμενο. Αυτό το ζήτημα μπορεί να περιπλέξει και να δημιουργήσει καθυστερήσεις στην καταγραφή των περιστατικών, διότι κάθε παραβίαση δεδομένων θα πρέπει να αποτυπωθεί ξεχωριστά, καθώς όλα τα είδη των προσωπικών δεδομένων που παραβιάστηκαν με διαφορετικούς τρόπους πρέπει να καταγράφονται μεμονωμένα[255].

Όσον αφορά τα big data, και δυνητικά ευαίσθητα στο πλαίσιο του IoT, η εκτίμηση των επιπτώσεων της επεξεργασίας (PIA) αποτελεί την έμπρακτη απόδειξη της συμμόρφωσης με τις αρχές του GDPR, πριν από τη λειτουργία κάθε νέας εφαρμογής IoT, με την ακόλουθη δημοσιοποίηση των αποτελεσμάτων της

[252] Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report*, *15*, 153.

[253] Loideain, N. N. (2019). A port in the data-sharing storm: the GDPR and the Internet of things. *Journal of Cyber Policy*, *4*(2), 178-196.

[254] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[255] Article 29 Working Party. (2018). "Guidelines on Personal data breach notification under Regulation 2016/679". Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

PIA[256]. Κατά τη διενέργεια της εκτίμησης του αντικτύπου σε περιβάλλον IoT, η οποία θα πρέπει να αντιμετωπιστεί ως μία νέα εξειδικευμένη προσέγγιση της PIA, μεταξύ των τρεχουσών γενικών εκτιμήσεων αντικτύπου[257], φέρει ως βασικούς πυλώνες: την ανάγκη για εξελισσόμενη και όχι μόνο περιοδική αξιολόγηση, τον συνδυασμό αυτοματοποιημένων αποφάσεων με εκείνες που λαμβάνονται με ανθρωπινή παρέμβαση, τα ενδεχόμενα νέα και «άγνωστα» συστήματα και τις εκάστοτε νομικές και κοινωνικές προκλήσεις[258].

Όσον αφορά την προστασία των δεδομένων από τον σχεδιασμό, αναμφίβολα ο στόχος της ασφάλειας σε περιβάλλοντα IoT, ειδικά με την εισβολή της τεχνολογίας 5G, καθίσταται μία περίπλοκη διαδικασία, η οποία απαιτεί την επέκταση του υπάρχοντος πρωτοκόλλου ασφαλείας[259]. Σε αυτήν την κατεύθυνση, έχει προταθεί ότι κατά τον σχεδιασμό της ανταλλαγής των δεδομένων στο IoT, ακόμα και όταν πρέπει να γίνει ταυτοποίηση των δεδομένων επιβεβλημένη από τον νόμο, θα πρέπει να σταθμιστεί η αναγκαιότητα της διαβίβασης όλων των δεδομένων που μπορεί να ανταλλάσσονται στο IoT, σύμφωνα με την αρχή της αναλογικότητας[260]. Επιπλέον, καθώς η ανάπτυξη του IoT θα πραγματοποιηθεί ως απόρροια της τεχνολογίας 5G, θα πρέπει να αναφερθεί η προσέγγιση ασφάλειας end-to-end, η οποία στρέφει την προσοχή στις έξυπνες συσκευές που είναι σε θέση να λαμβάνουν λεπτομερείς και εξουσιοδοτημένες αποφάσεις με βάση ένα συγκεκριμένο πλαίσιο και βασίζεται στην κρυπτογράφηση δημοσίου κλειδιού (public key cryptography)[261].

Όπως αναφέρθηκε ο συνδυασμός Iot-5G απαιτεί μια ολοκληρωμένη, συστηματική και συχνά αναθεωρούμενη στρατηγική ασφαλείας. Εκτός από τη μέθοδο της κρυπτογράφησης για την ασφάλεια των δεδομένων μέσα σε αυτό το

[256] Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016, September). A process for data protection impact assessment under the european general data protection regulation. In *Annual Privacy Forum* (pp. 21-37). Springer, Cham.

[257] Nurse, J. R., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. *IT professional*, *19*(5), 20-26.

[258] Nurse, J. R., Radanliev, P., Creese, S., & De Roure, D. (2018). If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems.

[259]5G PPP Architecture Working Group: *View on 5G Architecture*. (2019) 3rd edition. Διαθέσιμο στο: https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf

[260] Sanchez, J. L. C., Bernabe, J. B., & Skarmeta, A. F. (2018). Towards privacy preserving data provenance for the Internet of Things. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 41-46). IEEE.

[261] Skarmeta, A. F., Hernandez-Ramos, J. L., & Moreno, M. V. (2014). A decentralized approach for security and privacy challenges in the internet of things. In *2014 IEEE world forum on Internet of Things (WF-IoT)* (pp. 67-72). IEEE.

περιβάλλον, υπάρχουν και άλλες προσεγγίσεις στην ασφάλεια των δεδομένων. Ενδεικτικά: ασφάλεια της συσκευής (device security), ασφάλεια επικεντρωμένη στις υπηρεσίες (service-oriented security), αξιολόγηση της ασφάλειας (security assessment), ασφάλεια χαμηλής καθυστέρησης της κινητικότητας (low-delay mobility security), ασφάλεια του χρήστη (user protection))[262], οι οποίες στοχεύουν ως επί το πλείστον στην ελάχιστη δυνατή προσβασιμότητα.

4) ΕΞΑΡΤΗΣΗ ΑΠΟ IP:

Καταρχάς, οι ασύρματες τεχνολογίες και οι πάροχοι των υπηρεσιών στα δίκτυα 5G, οι οποίοι μετέχουν σε ένα κεντρικό δίκτυο βασισμένο σε IP, θα έχουν ως αποτέλεσμα εναλλασσόμενους παρόχους, βελτιώνοντας τη λειτουργικότητα των κινητών συσκευών και προκαλώντας προβλήματα σχετικά με τον έλεγχο πρόσβασης, την ασφάλεια των τηλεπικοινωνιών, την εμπιστευτικότητα και διαθεσιμότητα των δεδομένων[263]. Οι παράγοντες αυτοί περιπλέκουν τον σχεδιασμό της ασφάλειας, που βασίζεται κυρίως στην κρυπτογράφηση[264]. Ωστόσο, η παραδοσιακή μέθοδος της κρυπτογράφησης εμφανίζει ζητήματα αποτελεσματικότητας σε σχέση με την ανάλυση big data σε πραγματικό χρόνο[265].

Οι διευθύνσεις IP, οι οποίες αποτελούν προσωπικά δεδομένα, κατηγοριοποιούνται ως δεδομένα τοποθεσίας[266]. Οι διαδικτυακές υπηρεσίες που βασίζονται στην τοποθεσία (Location-based Internet services) αποτέλεσαν έναν καταλυτικό παράγοντα ανάπτυξης των υπηρεσιών καταγραφής δεδομένων τοποθεσίας, οι οποίες υπολογίζουν τη θέση του υποκειμένου των δεδομένων μίας διεύθυνσης IP[267]. Παρόλο που η καταγραφή της διεύθυνσης IP έχει

[262] Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1-9.

[263] Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, *101*, 55-82.

[264] Zhang, G., Fan, D., Zhang, Y., Li, X., & Liu, X. (2015). A privacy preserving authentication scheme for roaming services in global mobility networks. *Security and Communication Networks*, *8*(16), 2850-2859.

[265] Yin, C., Xi, J., Sun, R., & Wang, J. (2017). Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3628-3636.

[266] Bargiotti, L., Gielis, I., Verdegem, B., Breyne, P., Pignatelli, F., Smits, P., & Boguslawski, R. (2016). *Guidelines for public administrations on location privacy: European Union Location Framework* (No. JRC103110). Joint Research Centre (Seville site).

[267] Barnes, R., Winterbottom, J., & Dawson, M. (2011). Internet geolocation and location-based services. *IEEE Communications Magazine*, *49*(4), 102-108.

αντιμετωπιστεί στα πρωτόκολλα της τεχνολογίας 5G[268], μία επιπρόσθετη απαίτηση για την προστασία των δεδομένων είναι η εξασφάλιση της νόμιμης συλλογής προσωπικών δεδομένων τοποθεσίας (διεύθυνση IP). Για παράδειγμα, η συγκατάθεση για έναν σκοπό επεξεργασίας (Location-based Internet services), δεν μπορεί να παραμένει έγκυρη μετά την επίτευξη του αρχικού σκοπού[269]. Με την έλευση της τεχνολογίας 5G και τον αυξημένο αριθμό νέων συσκευών και της συνδεσιμότητας αυτών των συσκευών, είναι σημαντικό να διασφαλιστεί η ελαχιστοποίηση δεδομένων και ο περιορισμός αποθήκευσης των διευθύνσεων IP, καθώς αυτά τα δεδομένα θα αυξηθούν. Θα πρέπει, ακόμη, να διασφαλίζεται ότι κάθε φορά που απαιτείται επεξεργασία της διεύθυνσης IP τα δεδομένα τοποθεσίας δε θα χρησιμοποιούνται για άλλο σκοπό και για περισσότερο χρόνο από αυτόν που είναι απαραίτητος.

Η αποκάλυψη των δεδομένων θέσης μπορεί να προκαλέσει επίθεση εκτός του ψηφιακού περιβάλλοντος και εντός, όπως ανεπιθύμητη αλληλογραφία ή στοχευμένη διαφήμιση. Επίσης μπορεί να περιλαμβάνει τη δημιουργία προφίλ, μέσω της συλλογής δεδομένων μίας πολύ ακριβούς γεωγραφικής τοποθεσίας, τα οποία μπορούν να συνδεθούν με άλλα δεδομένα, αποκαλύπτοντας κατά συνέπεια επιπρόσθετα προσωπικά δεδομένα.

4.1.5 Ζητήματα ασφάλειας των δικτύων 5G και τεχνικές λύσεις που απορρέουν από τον GDPR

Γενικά, η ασφάλεια της επεξεργασίας των δεδομένων προϋποθέτει τη λήψη τεχνολογικών και οργανωτικών μέτρων[270], για τα οποία εξετάζεται κάθε φορά η σύγχρονη τεχνολογία, το κόστος, το είδος της επεξεργασίας και οι ενδεχόμενοι κίνδυνοι[271]. Εκτός από την περιγραφή στην ενότητα 4.1.3.2.2 των οργανωτικών μέτρων ασφάλειας, τα οποία προκύπτουν από το νόμο (γνωστοποίηση παραβίασης δεδομένων, εκτίμηση αντίκτυπου και προστασία των δεδομένων από τον σχεδιασμό), θα πρέπει να αναλυθούν τα τεχνολογικά μέτρα ασφαλείας των

[268] 3GPP, 3GPP TS 23.501: "System architecture for the 5G System (5GS)". Διαθέσιμο στο: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[269] Bargiotti, L., Gielis, I., Verdegem, B., Breyne, P., Pignatelli, F., Smits, P., & Boguslawski, R. (2016). *Guidelines for public administrations on location privacy: European Union Location Framework* (No. JRC103110). Joint Research Centre (Seville site).

[270] Council of Europe. (2018). *Handbook on European data protection law.* Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

[271] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (pp. 34-307). New York: John Wiley & Sons.

δικτύων 5G, δεδομένου ότι είναι εξειδικευμένα και καλύπτουν όλα τα χαρακτηριστικά των δικτύων. Η εισβολή των νέων υπηρεσιών και συσκευών θα επηρεάσει την ασφάλεια σε περιβάλλοντα 5G, δημιουργώντας ζητήματα στην προστασία της ιδιωτικότητας. Τα δίκτυα 5G, περικλείοντας έναν μεγάλο αριθμό συσκευών, δύνανται να εμφανίσουν νέα αναγνωριστικά χρήστη και συσκευών, όπως νέα αναγνωριστικά αποκλειστικά για IoT συσκευές[272].

Τα τεχνολογικά μέτρα ασφαλείας, όπως θεσπίζονται από τον GDPR, περιλαμβάνουν την ψευδωνυμοποίηση και την ανωνυμοποίηση (τα οποία αναφέρονται στην ενότητα 4.1.3.2.2) και τη μέθοδο της κρυπτογράφησης (αιτιολογική σκέψη 83, άρθρο 32). Οι διατάξεις του GDPR για την προστασία των προσωπικών δεδομένων δεν καλύπτουν τα ανώνυμα δεδομένα, τα οποία δεν σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (αιτιολογική σκέψη 26 σε συνδυασμό με το άρθρο 4 περ. 1). Όσον αφορά τα δεδομένα τα οποία έχουν υποστεί ψευδωνυμοποίηση, θεωρούνται ασφαλή, εάν δεν μπορούν να αποδοθούν σε ένα φυσικό πρόσωπο (αιτιολογική σκέψη 26), εφόσον, όμως, παραμένουν μη αναγνωρίσιμα σύμφωνα με τις τρέχουσες τεχνολογικές εξελίξεις, λαμβάνοντας επίσης υπόψη τον χρόνο και το κόστος της διαδικασίας ταυτοποίησης. Στο πλαίσιο της ασφάλειας των δικτύων 5G, ένας σημαντικός και αποτελεσματικός στόχος είναι ο διαχωρισμός του χρήστη μίας συσκευής από την ίδια τη συσκευή[273].

Η λύση για τα θέματα της ταυτοποίησης των χρηστών στα δίκτυα 5G που έχει διατυπώσει ο οργανισμός 3GPP[274] είναι η προστασία του μόνιμου αναγνωριστικού του χρήστη ενάντια σε ενεργές επιθέσεις χρησιμοποιώντας ένα δημόσιο κλειδί στο οικιακό δίκτυο[275]. Επιπλέον, εφόσον τα δίκτυα 5G απαιτούν αδιάκοπα (end-to-end) μέτρα ασφαλείας για την κάλυψη των απαιτήσεων GDPR,

---

[272] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (pp. 34-307). New York: John Wiley & Sons.

[273] Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security* (pp. 34-307). New York: John Wiley & Sons.

[274]Ο 3GPP είναι ο κύριος παγκόσμιος φορέας ανάπτυξης προτύπων για τις τηλεπικοινωνίες, αποτελώντας μία συνεργασία μεταξύ επτά οργανωτικών εταίρων, από την Ευρώπη (ETSI), τις ΗΠΑ (ATIS), την Κίνα (CCSA), την Ιαπωνία (ARIB, TTC), την Κορέα (TTA) και την Ινδία (TSDSI). Οι ομάδες δημιουργίας τεχνικών προδιαγραφών του 3GPP έχουν τυποποιήσει τα χαρακτηριστικά ασφαλείας για την βιομηχανία για τα πρότυπα που διέπουν τα 3G, 4G και 5G δίκτυα. Βλ. NIS Cooperation Group. (2020). Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Διαθέσιμο στο: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[275] Prasad, A. R., Zugenmaier, A., Escott, A. & Soveri, M. C. (2018). "3GPP 5G security". Διαθέσιμο στο : http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g?from=timeline

τα πρότυπα του 3GPP για τα δίκτυα 5G ορίζουν ότι τα αναγνωριστικά των χρηστών κρυπτογραφούνται κατά τη μετάδοση μέσω της διεπαφής αέρος (air interface), η κρυπτογράφηση και η προστασία της ακεραιότητας διενεργούνται στον δίαυλο μετάδοσης (transmission channel) end-to-end[276], για τη διασφάλιση των προσωπικών δεδομένων από τυχαία, μη εξουσιοδοτημένη ή παράνομη πρόσβαση, χρήση, τροποποίηση, αποκάλυψη, απώλεια, καταστροφή ή ζημία (αιτιολογική σκέψη 39 και άρθρο 5 παρ.1).

Οι απαιτήσεις ασφάλειας και προστασίας των προσωπικών δεδομένων που έχει θέσει η Ομάδα Εργασίας SA3[277] του 3GPP στις προδιαγραφές που τίθενται στο 3GPP TS 33.501 για τα δίκτυα 5G είναι: (α) η εμπιστευτικότητα των δεδομένων των χρηστών και των δεδομένων σήματος, (β) η ακεραιότητα των δεδομένων των χρηστών και των δεδομένων σήματος, (γ) η ασφαλής αποθήκευση και επεξεργασία των διαπιστευτηρίων της εγγραφής και (δ) η ιδιωτικότητα του χρήστη[278]. Θα πρέπει να αναφερθεί ότι τα παραπάνω στοιχεία της ασφάλειας δεν ενεργοποιούνται εν όλω από τον σχεδιασμό του εξοπλισμού του δικτύου, καθώς ορισμένα από αυτά εφαρμόζονται προαιρετικά από τους παρόχους ή τους φορείς εκμετάλλευσης. Ως εκ τούτου, η αποτελεσματικότητα αυτών των απαιτήσεων ασφάλειας εξαρτάται από τον τρόπο με τον οποίο οι φορείς εκμετάλλευσης θέτουν σε εφαρμογή και διαχειρίζονται τα δίκτυά τους[279]. Το Ευρωπαϊκό Συμβούλιο έχει διατυπώσει την ανάγκη θέσπισης ισχυρών κοινών προτύπων και μέτρων ασφάλειας, με έμφαση στην προστασία των προσωπικών δεδομένων από το σχεδιασμό, λαμβάνοντας υπόψη τα διεθνή πρότυπα των δικτύων 5G[280].

---

[276] Partnering with the Industry for 5G Security Assurance. (2019). Huawei White Paper, Shenzhen, China.

[277] Η Ομάδα Εργασίας SA3 (Service and System Aspects 3 Working Group) είναι υπεύθυνη για την ασφάλεια και την προστασία των προσωπικών δεδομένων στα πρότυπα που διέπουν τα δίκτυα 5G. Βλ. NIS Cooperation Group. (2020). Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Διαθέσιμο στο: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[278] 3GPP, 3GPP TS 33.501: Security architecture and procedures for 5G System. Διαθέσιμο στο: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[279] NIS Cooperation Group. (2020). Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Διαθέσιμο στο: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[280] Council of the European Union. (2019). Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G-Council Conclusions (14517/19). Brussels. Διαθέσιμο στο: https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/

Επιπλέον, όπως καταγράφθηκαν από την Ομάδα Συνεργασίας NIS[281], οι απαιτήσεις για τα κράτη μέλη της ΕΕ είναι: (α) η αύξηση των μέτρων ασφαλείας για τους φορείς εκμετάλλευσης των δικτύων κινητής τηλεφωνίας 5G, (β) η εφαρμογή περιορισμών για τους παρόχους υψηλού κινδύνου, βασιζόμενων σε μία υποβληθείσα εκτίμηση του κινδύνου και (γ) η διασφάλιση της ύπαρξης πολλαπλών παρόχων για τους φορείς εκμετάλλευσης, προκειμένου να αποφεύγεται οποιαδήποτε εξάρτηση από έναν μόνο πάροχο και ιδίως από έναν πάροχο υψηλού κινδύνου.

Καταλήγοντας, τα μέτρα ασφαλείας για την τεχνολογία 5G που απορρέουν από τον GDPR, που δύνανται να εφαρμοστούν, περιλαμβάνουν την ανωνυμοποίηση, την ψευδωνυμοποίηση και γενικότερα την προστασία των προσωπικών δεδομένων από τον σχεδιασμό, με στόχο να διατηρείται η αδιάκοπη (end-to-end) και η ad hoc προστασία των δεδομένων[282].

4.1.6 Συμπερασματικές παρατηρήσεις

Η παρούσα ενότητα πραγματεύεται την αλληλεπίδραση μεταξύ της τεχνολογίας 5G και του GDPR, βασιζόμενη σε αρχές, προκειμένου να επιστήσει την προσοχή σε συγκεκριμένα στοιχεία, στοχεύοντας στην εκπόνηση μίας βασικής ταξινόμησης με βάση τα δικαιώματα και τις υποχρεώσεις του GDPR. Είναι αξιοσημείωτη η διευκρίνιση ότι η καταγραφείσα αλληλεπίδραση, όπως αποτυπώνεται και στον Πίνακα 1, έχει ποιοτική σημασία, καθώς κάθε σημείο επαφής έχει μία ιδιαίτερη αυτοτέλεια, η οποία θα μπορούσε να αποτελέσει αντικείμενο για μελλοντική έρευνα.

Επίσης, αυτή η ερευνητική εργασία διακρίνει τα πιο σημαντικά στην πράξη δικαιώματα και μέτρα ασφαλείας του GDPR, τα οποία σχετίζονται άμεσα με τις αρχές και τις υποχρεώσεις του GDPR, συνδέοντάς τα με τα ασύρματα δίκτυα 5^{ης} γενιάς.

Πιο συγκεκριμένα, παρουσιάστηκε η ανάλυση του πεδίου της προστασίας των δεδομένων στο νομικό σύστημα της ΕΕ, μέσα σε IoT περιβάλλον υπό το πρίσμα των δικτύων 5G, η οποία αναδεικνύει ζητήματα σχετικά με τα περισσότερα δικαιώματα και τις αρχές του GDPR, καθιστώντας απαραίτητη την

[281] NIS Cooperation Group. (2020). Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Διαθέσιμο στο: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[282] Council of Europe. (2018). *Handbook on European data protection law*. Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

ευαισθητοποίηση σε επίπεδο έρευνας με την εισβολή των έξυπνων πόλεων και εκατομμυρίων φορητών συσκευών. Η προστασία της ιδιωτικότητας δεν τελεσφορεί μόνο στην προσπάθεια αποφυγής των διοικητικών προστίμων εκατομμυρίων ευρώ, αλλά και στην προσπάθεια δημιουργίας μίας δίκαιης και ολοκληρωμένης αντιμετώπισης για τα δικαιώματα προστασίας των δεδομένων από την απαρχή της τεχνολογίας 5G.

Αυτή η μελέτη αποσκοπεί στην ανάδειξη της ανάγκης γεφύρωσης του τεχνολογικού και νομικού κλάδου στο πλαίσιο των προκλήσεων των επιπτώσεων της τεχνολογίας 5G στο πλαίσιο του GDPR.

4.2 Τα αναδυόμενα δίκτυα νέας γενιάς 6G

4.2.1 Ταξινόμηση της αυτοματοποιημένης λήψης αποφάσεων σύμφωνα με τον GDPR στα αναδυόμενα δίκτυα 6G[283]

(Δημοσιεύθηκε στα Πρακτικά του 3rd World Symposium on Communication Engineering (WSCE) 2020, IEEE, doi: 10.1109/WSCE51339.2020.9275570)

4.2.2 Εισαγωγή

Η αυτοματοποιημένη λήψη αποφάσεων και η δημιουργία προφίλ εξαπλώνονται ταχύτατα σε όλους τους τομείς της σύγχρονης ζωής, όπως στο ηλεκτρονικό εμπόριο, στον χρηματοπιστωτικό τομέα, στο μάρκετινγκ και στον τομέα των μεταφορών. Οι συνεχώς αυξανόμενες δυνατότητες της αυτοματοποιημένης επεξεργασίας, οι οποίες προκύπτουν από τις νέες τεχνολογίες (όπως τα επερχόμενα δίκτυα κινητής τηλεφωνίας 6G), δημιουργούν την ανάγκη εξειδικευμένης προστασίας των δεδομένων. Το αντικείμενο της παρούσας ενότητας είναι η παρουσίαση μίας ταξινόμησης και των αντίστοιχων θεσμικών προτάσεων, οι οποίες στοχεύουν στην ανάδειξη των επιπτώσεων του δικαιώματος

[283] Η παρούσα ενότητα του κεφαλαίου δημοσιεύθηκε ως ερευνητική εργασία στην αγγλική γλώσσα στα Πρακτικά του 3rd World Symposium on Communication Engineering (WSCE) 2020 υπό τον τίτλο:
Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020, October). Taxonomy about the Stages of Performing Automated Decision-Making Processing under GDPR in the Light of 6G Networks. In *2020 3rd World Symposium on Communication Engineering (WSCE)* (pp. 23-27). IEEE.

Η ερευνητική εργασία υποστηρίχθηκε από το Ελληνικό Ίδρυμα Έρευνας και Καινοτομίας (ΕΛΙ.Δ.Ε.Κ.) στο πλαίσιο της Δράσης «Υποτροφίες ΕΛΙ.Δ.Ε.Κ. Υποψηφίων Διδακτόρων» (Αριθμός Υποτροφίας: 290)

του άρθρου 22 του GDPR, ιδιαίτερα μετά τη σύμπλευση των δικτύων 6G με την τεχνητή νοημοσύνη (AI).

4.2.2.1 Ο ρόλος της τεχνητής νοημοσύνης στα δίκτυα 6G

Η αυτοματοποιημένη λήψη αποφάσεων επιτυγχάνεται μέσω αλγορίθμων ή συστημάτων AI [284]. Η τεχνητή νοημοσύνη (AI) είναι η νοημοσύνη που αναπτύχθηκε από τον άνθρωπο και χρησιμοποιείται ως τεχνικό εργαλείο του[285]. Πιο συγκεκριμένα, οι μηχανές λειτουργούν σαν «έξυπνοι πράκτορες (intelligent agents)», οι οποίοι ενεργούν σύμφωνα με αλγόριθμους και το περιβάλλον τους με την υποστήριξη λογισμικού[286] [287].

Ο αλγόριθμος περιλαμβάνει τις διαδικασίες του υπολογισμού, της επεξεργασίας δεδομένων, της αξιολόγησης και της αυτοματοποιημένης συλλογιστικής και λήψης αποφάσεων. Ως εκ τούτου, η τεχνητή νοημοσύνη που περιλαμβάνει τη μηχανική μάθηση, απαιτεί την παραγωγή, συλλογή και επεξεργασία (π.χ. δημιουργία προφίλ[288]) δεδομένων μεγάλης κλίμακας (big data)[289]. Ο τρόπος με τον οποίο ενεργεί ένας αλγόριθμος κυμαίνεται μεταξύ καθολικά αυτοματοποιημένων και εν μέρει αυτοματοποιημένων αποφάσεων[290]. Ο

[284] Araujo, T., Helberger, N., Kruikemeier, S., & De Vreese, C. H. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & SOCIETY*, *35*(3), 611-623.

[285] Korb, K. B., & Nicholson, A. E. (2010). *Bayesian artificial intelligence*. CRC press.

[286] Russell, S. J., & Norvig 2nd, P. (2003). edn: Artificial Intelligence: A Modern Approach. pp. 27, 32–58, 968–972.

[287] Russell Stuart, J., & Norvig, P. (2009). *Artificial intelligence: a modern approach*. Prentice Hall. p.2

[288] «κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου. (Άρθρο 4 περ. 4 GDPR)

[289] Council of Europe. (2018). *Handbook on European data protection law.* Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

[290] Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, *24*(10), 1572-1593.

GDPR δεν επιτρέπει τις αποφάσεις που βασίζονται «αποκλειστικά σε αυτοματοποιημένη επεξεργασία»[291].

Η συνεχιζόμενη άνοδος της AI θα υποστηρίζεται από διαφορετικές νέες τεχνολογίες, όπως τα επερχόμενα δίκτυα 6G (έκτη γενιά ασύρματων κυψελοειδών συστημάτων), στα οποία θα αποτελεί βασική απαίτηση η υποστήριξη εφαρμογών AI από τον πυρήνα τους έως και τις τελικές συσκευές[292]. Η ενότητα παρουσιάζει μια ταξινόμηση η οποία μπορεί να χρησιμοποιηθεί για τη διεξαγωγή μίας αυτοματοποιημένης λήψης αποφάσεων, διαφυλάσσοντας την προστασία αφενός των υποκειμένων των δεδομένων που βρίσκονται στον ΕΟΧ και αφετέρου των υποκείμενων των δεδομένων που βρίσκονται εκτός του ΕΟΧ, όταν η επεξεργασία σχετίζεται με τις λειτουργίες του εκτελούντα ή υπεύθυνου της επεξεργασίας που βρίσκεται εντός της ΕΟΧ[293].

4.2.2.2 Τα στάδια της αυτοματοποιημένης λήψης αποφάσεων σύμφωνα με το άρθρο 22 του GDPR

1) Πρώτο στάδιο - Ανωνυμοποίηση

Το μέτρο ασφάλειας της ανωνυμοποίησης[294] θα μπορούσε να καταστήσει δυνατή την αποφυγή όλων των επόμενων σταδίων υπό ορισμένες προϋποθέσεις, όπως παρουσιάζεται και στο Γράφημα 2. Αναλυτικότερα, οι αρχές του GDPR δεν εφαρμόζονται στα ανώνυμα δεδομένα τα οποία δεν σχετίζονται με ένα

[291] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[292] Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y. J. A. (2019). The roadmap to 6G: AI empowered wireless networks. *IEEE Communications Magazine*, *57*(8), 84-90.

[293] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[294] Η «ανωνυμοποίηση» είναι μια τεχνική η οποία εφαρμόζεται, σύμφωνα με τα σύγχρονα τεχνολογικά μέσα, στα προσωπικά δεδομένα, προκειμένου να τα μετατρέψει σε μη προσωπικά. Βλ. Article 29 Data Protection Working Party. (2014). "Opinion 05/2014 on Anonymisation Techniques".WP216. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή δεν μπορούν να συμβάλλουν στην εξακρίβωση της ταυτότητας του προσώπου (αιτιολογική σκέψη 26 σε συνδυασμό με το άρθρο 4 περ. 1). Πρέπει να αναφερθεί, ωστόσο, ότι η ανωνυμοποίηση είναι μια συνεχής διαδικασία, η οποία ακολουθεί την εξέλιξη της τεχνολογίας, και πρέπει να επανεξετάζεται και να αναθεωρείται ανά τακτά χρονικά διαστήματα από τους υπεύθυνους της επεξεργασίας των δεδομένων προκειμένου να αποφευχθεί η ταυτοποίηση των φυσικών προσώπων[295]. Επιπλέον, όσον αφορά την ύπαρξη συνόλου δεδομένων (datasets) τα οποία αποτελούνται από συνδεδεμένα προσωπικά και μη δεδομένα, ο GDPR ισχύει για όλα τα δεδομένα αυτών των μικτών συνόλων δεδομένων. Τα μικτά σύνολα δεδομένων αποτελούν αναμφισβήτητα και την πιο συνήθη περίπτωση, ειδικά στο πλαίσιο του IoT και της AI[296].

2) Δεύτερο στάδιο- Δικαιώματα του υποκειμένου των δεδομένων

Όπως σε κάθε επεξεργασία δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων είναι τα ακόλουθα[297]:

1) Δικαίωμα ενημέρωσης (άρθρο 13,14)

2) Δικαίωμα πρόσβασης (άρθρο 15)

3) Δικαίωμα διόρθωσης (άρθρο 16)

4) Δικαίωμα διαγραφής/λήθης (άρθρο 17)

5) Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18)

6) Δικαίωμα γνωστοποίησης σχετικά με την διαγραφή, διόρθωση ή τον περιορισμό (άρθρο 19)

7) Δικαίωμα στη φορητότητα των δεδομένων (άρθρο 20)

---

[295] Council of Europe, Consultative Committee of Convention 108. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01. Strasbourg. Διαθέσιμο στο: https://rm.coe.int/16806ebe7a

[296] European Commission. (2019). Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union. Brussels. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN

[297] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

8) Δικαίωμα εναντίωσης (άρθρο 21)

9) Δικαίωμα στην ανθρώπινη παρέμβαση (άρθρο 22), το οποίο παρουσιάζεται αυτοτελώς και αναλυτικότερα στο παρακάτω τρίτο στάδιο.

3) Τρίτο στάδιο - Δικαίωμα στην ανθρώπινη παρέμβαση (άρθρο 22)

Α) Ενήλικες

Καταρχάς, η επεξεργασία προσωπικών δεδομένων που περιλαμβάνει αυτοματοποιημένη λήψη αποφάσεων και έχει νομική ή παρόμοια σημαντική επίδραση, συμπεριλαμβανομένης της κατάρτισης προφίλ, απαγορεύεται από τον GDPR[298], και επιτρέπεται μόνο σε περίπτωση:

α) ρητής συγκατάθεσης του υποκειμένου των δεδομένων,

β) ύπαρξης σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας των δεδομένων και

γ) υποστήριξης από το δίκαιο των κρατών μελών ή το δίκαιο της ΕΕ[299].

Η συγκατάθεση στο πλαίσιο του άρθρου 22 του GDPR θα πρέπει να είναι ρητή, εν πλήρει επιγνώσει (δοθείσα ενημέρωση σχετικά με τη χρήση των προσωπικών δεδομένων για την αυτοματοποιημένη λήψη αποφάσεων), ελεύθερη, συγκεκριμένη, και σαφής[300]. Ως προς την περίπτωση ύπαρξης σύμβασης, η αυτοματοποιημένη λήψη αποφάσεων μπορεί επίσης να εκτελείται κατά το προσυμβατικό στάδιο[301]. Η περίπτωση (γ) αναφέρεται στην ύπαρξη σχετικού νόμου, εθνικού ή ενωσιακού, ο οποίος να επιτρέπει την αυτοματοποιημένη διαδικασία λήψης αποφάσεων (πχ. παρακολούθηση της απάτης και της φοροδιαφυγής σύμφωνα με την αιτιολογική σκέψη 71) .

Β) Παιδιά

---

[298] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[299] Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report*, *15*, 153.

[300] EDPB (European Data Protection Board). (2020). Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.0. Διαθέσιμο στο: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[301] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Οι παραπάνω εξαιρέσεις (α), (β), (γ) που επιτρέπουν την αυτοματοποιημένη λήψη αποφάσεων, διαφοροποιούνται σε μεγάλο βαθμό όταν πρόκειται για επεξεργασία που αφορά παιδιά, σύμφωνα με την αιτιολογική σκέψη 71[302] του GDPR , αναδεικνύοντας την ανάγκη για την ειδική προστασία τους.

Σύμφωνα με την ομάδα εργασίας του άρθρου 29[303], προκειμένου να εκτελεστεί επεξεργασία των προσωπικών δεδομένων παιδιών μέσω αυτοματοποιημένης λήψης αποφάσεων, θα πρέπει τα παραπάνω στοιχεία (α), (β), (γ) παράλληλα να στοχεύουν στην προστασία των δικαιωμάτων, των ελευθεριών και των εννόμων συμφερόντων των παιδιών[304]. Θα πρέπει να αναφερθεί ότι, όσον αφορά τη συγκατάθεση των παιδιών, υπό τις προϋποθέσεις[305] του άρθρου 8 παρ. 1, υπάρχουν δύο περιπτώσεις με βάση την ηλικία τους:

α) 16 ετών και άνω

β) κάτω των 16 ετών.

Κατά την πρώτη περίπτωση, αρκεί η συγκατάθεση του ανηλίκου ηλικίας 16 ετών και άνω, ενώ στη δεύτερη περίπτωση είναι απαραίτητη η γονική συγκατάθεση ή η γονική έγκριση της συγκατάθεσης των ανηλίκων[306]. Πιο συγκεκριμένα, οι εθνικές δικαιοδοσίες δύνανται να ορίζουν, όπως στην περίπτωση μίας ευρωπαϊκής Οδηγίας, το ηλικιακό όριο για τη γονική συγκατάθεση ή έγκριση, με γενικό κατώτατο όριο την ηλικία των 13 ετών[307].

4) Αυτοματοποιημένη λήψη αποφάσεων των ευαίσθητων προσωπικών δεδομένων

[302] «…*Το εν λόγω μέτρο θα πρέπει να μην αφορά παιδί*.» Βλ. Αιτιολογική σκέψη 71 GDPR

[303] Η ομάδα εργασίας του άρθρου 29 ήταν ένας ανεξάρτητος ευρωπαϊκός συμβουλευτικός φορέας για την προστασία των δεδομένων και την προστασία της ιδιωτικής ζωής, ο οποίος ιδρύθηκε βάσει της οδηγίας 95/46 / ΕΚ. Βλ. https://ec.europa.eu/newsroom/article29/news-overview.cfm

[304] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[305] «…*σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε παιδί*…». Βλ. Άρθρο 8 παρ. 1 GDPR

[306] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679. *ΔΙΜΕΕ, 1*, 5-19.

[307] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR interference with next generation 5G and IoT networks. *IEEE Access*, *8*, 108052-108061.

Η περίπτωση αυτοματοποιημένης λήψης αποφάσεων ευαίσθητων προσωπικών δεδομένων[308], μπορεί να πραγματοποιηθεί βάσει των διασφαλίσεων του άρθρου 22 του GDPR οι οποίες αναφέρθηκαν παραπάνω, σε συνδυασμό με μία από τις ακόλουθες διασφαλίσεις:

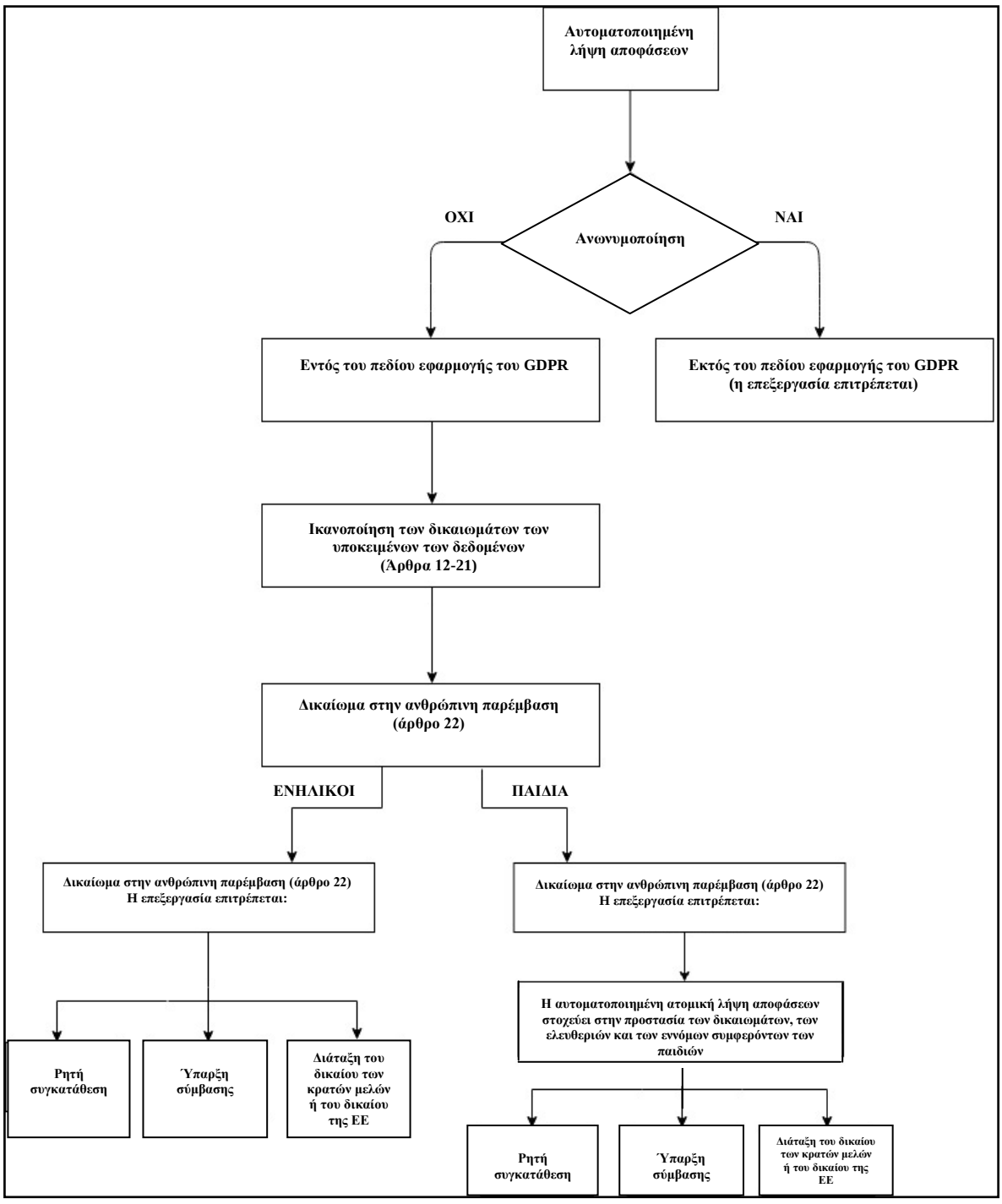
α) ρητή συγκατάθεση του υποκειμένου των δεδομένων (άρθρο 9 παρ. 2 περ. α, ή

β) απαραίτητη επεξεργασία για λόγους ουσιαστικού δημοσίου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων (άρθρο 9 παρ. 2 περ. ζ).

Παράλληλα, θα πρέπει να επιβάλλονται από τους υπευθύνους επεξεργασίας των δεδομένων κατάλληλα μέτρα, προκειμένου να διασφαλίζονται τα δικαιώματα, οι ελευθερίες και τα έννομα συμφέροντα του υποκειμένου των δεδομένων[309].

[308] «ευαίσθητα δεδομένα» είναι τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό. Βλ. Άρθρο 9 παρ. 1 GDPR.

[309] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053



Εικόνα 4.Τα στάδια της αυτοματοποιημένης διαδικασίας λήψης αποφάσεων σύμφωνα με το άρθρο 22 του GDPR

4.2.3 Προτάσεις σχετικά με τα ζητήματα ασφάλειας στα δίκτυα 6G

Αυτή η ενότητα περιλαμβάνει προτάσεις για τη θεσμοθέτηση και τη δημιουργία προτύπων για τα δίκτυα 6G, λαμβάνοντας υπόψη και την ταξινόμηση που παρουσιάζεται στην Εικόνα 4, με σκοπό να αναδείξει τα κρίσιμα ζητήματα της προστασίας των προσωπικών δεδομένων.

Α. Ανωνυμοποίηση των προσωπικών δεδομένων

Η σημασία της διατήρησης της ανωνυμίας των δεδομένων, ως μέτρο ασφαλείας εντός του περιβάλλοντος των δικτύων 6G, είναι ιδιαίτερα σημαντική, όπως προαναφέρθηκε παραπάνω. Η ανωνυμοποίηση δύναται εν γένει να καταστήσει δυνατή κάθε επεξεργασία δεδομένων, συμπεριλαμβανομένης της αυτοματοποιημένης λήψης αποφάσεων.

Β. AI (Αυτοματοποιημένη λήψη αποφάσεων)

Η επερχόμενη τεχνολογική ανάπτυξη και η θέση σε εφαρμογή των δικτύων 6G πρόκειται να συμπορευτούν παράλληλα με την τεχνητή νοημοσύνη. Πιο συγκεκριμένα, η δημιουργία προτύπων, η αρχιτεκτονική και τα χαρακτηριστικά των δικτύων 6G θα επηρεαστούν από τις εξελίξεις στην τεχνητή νοημοσύνη[310]. Ως αποτέλεσμα, η δημιουργία προτύπων και η ρύθμιση των μέτρων προστασίας της ιδιωτικής ζωής και της ασφάλειας στα δίκτυα 6G θα πρέπει να περιλαμβάνουν τα ζητήματα σχετικά με τη νόμιμη αυτοματοποιημένη επεξεργασία δεδομένων κατά τη λήψη αποφάσεων, όπως παρουσιάζεται στην προηγούμενη ενότητα. Αντιστοίχως, η προστασία των δεδομένων των παιδιών είναι εξαιρετικά σημαντική, όσον αφορά την χρήση AI στο περιβάλλον των δικτύων 6G. Καταρχήν, τα παιδιά θα πρέπει να αποκλείονται από τη διαδικασία δημιουργίας προφίλ, καθώς είναι ευάλωτα[311] [312], και ως εκ τούτου περισσότερο εκτεθειμένα απέναντι σε μεθόδους μάρκετινγκ.

Γ. Οι αρχές επεξεργασίας «περιορισμού της περιόδου αποθήκευσης», «περιορισμού του σκοπού» και της «ελαχιστοποίησης των δεδομένων»:

[310] Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y. J. A. (2019). The roadmap to 6G: AI empowered wireless networks. *IEEE Communications Magazine*, *57*(8), 84-90.

[311] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[312] Article 29 Working Party. (2013). "Opinion 02/2013 on apps on smart devices". WP202. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/news-overview.cfm

Σύμφωνα με την [313] ερευνητική εργασία, τα δίκτυα 6G θα εστιάζουν σε βελτιωμένη σχέση με το δίκτυο συγκριτικά με την τεχνολογία 5G. Ως αποτέλεσμα, λαμβάνοντας επίσης υπόψη την ανάπτυξη της τεχνητής νοημοσύνης, οι παράγοντες που μπορούν να επηρεάσουν την προστασία των προσωπικών δεδομένων και πρέπει να συνεκτιμηθούν κατά τη διαδικασία της δημιουργίας προτύπων στα δίκτυα 6G είναι οι εξής: ο χρόνος, η τοποθεσία, η χρήση και το πλαίσιο της εκάστοτε επεξεργασίας προσωπικών δεδομένων[314].

Πιο συγκεκριμένα, όσον αφορά τον χρόνο, η βασική πρόκληση είναι η συμμόρφωση με την αρχή επεξεργασίας, η οποία απαιτεί την περιορισμένη χρονική διάρκεια της διατήρησης των προσωπικών δεδομένων σε σχέση με μία συγκεκριμένη επεξεργασία «περιορισμός της περιόδου αποθήκευσης» (άρθρο 5 παρ. 1 περ. ε). Αναφορικά με την περίπτωση της χρήσης και το πλαίσιο της επεξεργασίας των δεδομένων, η προσοχή θα πρέπει να στραφεί και στις αρχές επεξεργασίας του «περιορισμού του σκοπού» (άρθρο 5 παρ. 1 περ. β) και της «ελαχιστοποίησης των δεδομένων» (άρθρο 5 παρ. 1 περ. γ). Αναλυτικότερα, η περίπτωση της χρήσης των προσωπικών δεδομένων θα πρέπει να είναι συγκεκριμένη, σύμφωνα με την αρχή του περιορισμού του σκοπού, καθιστώντας την περαιτέρω επεξεργασία και τη διατήρηση δεδομένων ασυμβίβαστη με τον πρωταρχικό σκοπό συλλογής[315]. Επιπρόσθετα, ως προς το πλαίσιο επεξεργασίας, θα πρέπει να εφαρμόζεται η αρχή της ελαχιστοποίησης των δεδομένων εξετάζοντας το πλαίσιο και τη χρήση κάθε επεξεργασίας μέσα σε δίκτυα 6G, προκειμένου να εκτελείται επεξεργασία μόνο στα απαραίτητα και ορθώς διατηρούμενα προσωπικά δεδομένα.

Δ. Ιδιωτικότητα σχετιζόμενη με την τοποθεσία

Τα δίκτυα 6G, εκτός από την ενεργοποίηση πολλών νέων εφαρμογών, αναμένεται να καταστήσουν δυνατή την υψηλή ακρίβεια ως προς τα δεδομένα θέσης[316], επιτυγχάνοντας ακρίβεια εντοπισμού των δεδομένων θέσης σε επίπεδο

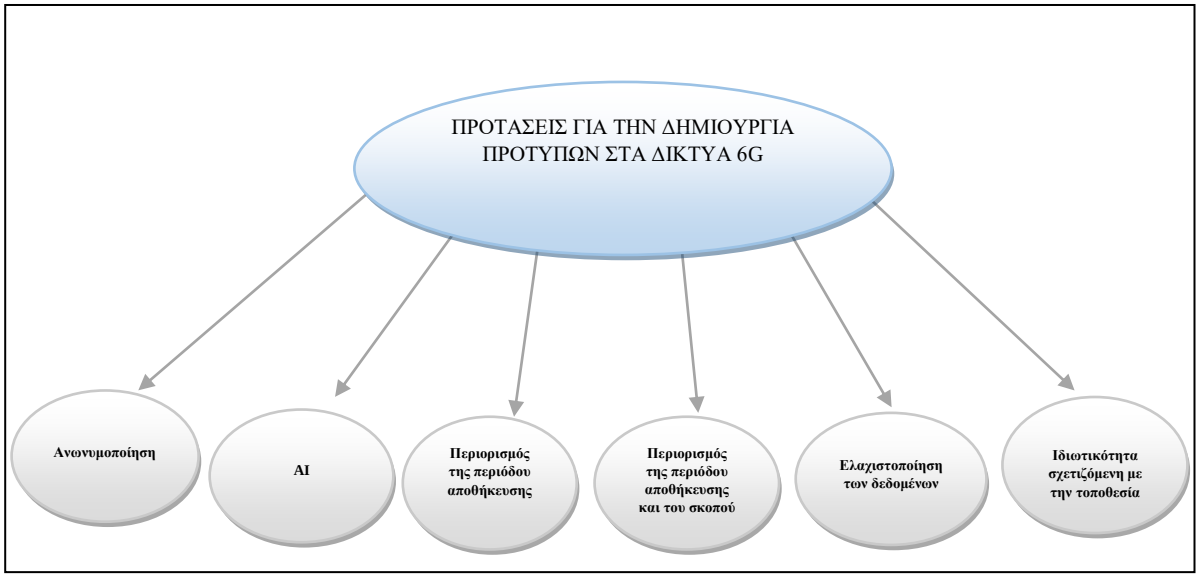
[313] Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., Hewa, T., Liyanage, M. & Ijaz, A. (2020). 6g white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*.

[314] Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., Hewa, T., Liyanage, M. & Ijaz, A. (2020). 6g white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*.

[315] Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report*, *15*, 153.

[316] Latva-aho, M., Leppänen, K., Clazzer, F., & Munari, A. (2020). Key drivers and research challenges for 6G ubiquitous wireless intelligence.

εκατοστών[317]. Επομένως, η ανάδειξη της ύπαρξης των ακριβέστερων δεδομένων θέσης σε πραγματικό χρόνο απαιτεί την εξειδικευμένη προστασία και ασφάλεια των δεδομένων. Επιπλέον, εκτός από το ζήτημα της συλλογής των δεδομένων θέσης (π.χ. μέσω μίας εφαρμογής), θα πρέπει να αξιολογηθεί σε επίπεδο δημιουργίας προτύπων και από τις οντότητες η αποφυγή του συνεχιζόμενου διαμοιρασμού των δεδομένων θέσης σε τρίτα μέρη (πχ. διαφημιστές, άλλες εφαρμογές)[318].



Εικόνα 5. Προτάσεις σχετικά με την προστασία της ιδιωτικότητας υπό το πρίσμα των δικτύων 6G

4.2.4 Συμπερασματικές παρατηρήσεις

Η ενότητα 4.2 αποσκοπεί στην ανάδειξη και επισήμανση μίας ταξινόμησης σχετικά με τα κύρια βασικά στάδια για την ορθή διαχείριση της αυτοματοποιημένης επεξεργασίας αποφάσεων, σύμφωνα με το δικαίωμα του υποκειμένου των δεδομένων του άρθρου 22 του GDPR. Επιπλέον, λαμβάνοντας υπόψη το αναδυόμενο πλαίσιο λειτουργίας των δικτύων 6G και την αλληλεπίδρασή τους με την τεχνολογία AI, καταγράφονται προτάσεις για την

[317] Xiao, Z., & Zeng, Y. (2020). An overview on integrated localization and communication towards 6G. *arXiv preprint arXiv:2006.01535*.

[318] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

προστασία της ιδιωτικής ζωής, όσον αφορά τη δημιουργία προτύπων στα δίκτυα 6G.

Ειδικότερα, είναι αξιοσημείωτη η αναφορά της σημασίας του συνδυασμού των νομικών εγγυήσεων στο πλαίσιο του άρθρου 22 και η διάκριση μεταξύ παιδιών και ενηλίκων αναφορικά με το δικαίωμα του υποκειμένου να μην υπόκεινται τα δεδομένα του σε αυτοματοποιημένη επεξεργασία.

Η ενότητα 4.2 απεικονίζει το πρότυπο της ΕΕ για την προστασία των δεδομένων σε ό,τι αφορά το δικαίωμα στην ανθρώπινη παρέμβαση και στρέφει την προσοχή στα κρίσιμα ζητήματα ιδιωτικότητας των δικτύων 6G, λαμβάνοντας υπόψη την τεχνητή νοημοσύνη. Παράλληλα, απώτερος στόχος αποτελεί η υποστήριξη των εμπλεκόμενων μερών τα οποία εκτελούν ή σχεδιάζουν την αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων.

ΚΕΦΑΛΑΙΟ 5. Η ΔΙΑΦΥΛΑΞΗ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΤΩΝ ΑΝΗΛΙΚΩΝ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ GDPR, ΣΤΑ ΕΞΥΠΝΑ ΣΠΙΤΙΑ ΠΟΥ ΒΑΣΙΖΟΝΤΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IoT), ΛΑΜΒΑΝΟΝΤΑΣ ΥΠΟΨΗ ΔΙΑΣΥΝΟΡΙΑΚΑ ΖΗΤΗΜΑΤΑ[319]

5.1 Προοίμιο

Εκτός από τις θετικές επιπτώσεις που δύνανται να επιφέρουν οι έξυπνες κατοικίες (smart homes) στον τομέα της οικονομίας, της ενέργειας, της ασφάλειας, καθώς και τα πλεονεκτήματα αποδοτικότητας και αξιοπιστίας που διαθέτουν, θα πρέπει παράλληλα να δοθεί προσοχή στις νομικές, δεοντολογικές και κοινωνικές συνέπειες των εν λόγω συστημάτων της τεχνολογίας της πληροφορίας. Ο τομέας της προστασίας των δεδομένων των παιδιών συναντά προκλήσεις, καθώς καθίστανται πιο ευάλωτα σε διαδικτυακούς κινδύνους και, ως εκ τούτου, η προστασία τους απαιτεί ένα εξειδικευμένο πλαίσιο διατήρησης της ιδιωτικότητάς τους. Το παρόν κεφάλαιο επιχειρεί να αναδείξει τα καίρια ζητήματα της προστασίας των δεδομένων των ανηλίκων, μέσω της προσέγγισης του ευρωπαϊκού δικαίου, σε σχέση με τις συσκευές που βασίζονται στο IoT σε ένα έξυπνο οικιακό περιβάλλον.

5.2 Εισαγωγικές παρατηρήσεις

Σε γενικές γραμμές, τα έξυπνα σπίτια, τα οποία συνίστανται από εφαρμογές του IoT[320], ορίζονται ως «κατοικία που ενσωματώνει ένα δίκτυο επικοινωνίας που συνδέει βασικές ηλεκτρικές συσκευές και υπηρεσίες που τους επιτρέπει να ελέγχονται, να εποπτεύονται ή να παρέχουν πρόσβαση εξ αποστάσεως» [321]. Ως εκ τούτου, διαφαίνεται ότι τα στοιχεία των έξυπνων σπιτιών (εξοπλισμός και συσκευές) δύνανται να αλληλεπιδρούν έξυπνα με όλα τα μέλη του

[319] Το παρόν κεφάλαιο δημοσιεύθηκε ως ερευνητική εργασία στην αγγλική γλώσσα στο επιστημονικό περιοδικό *Journal of Communications* υπό τον τίτλο:
Rizou, S., Alexandropoulou-Egyptiadou, E., Ishibashi, Y. & Psannis, K. E. (2022). Preserving Minors' Data Protection in IoT-based Smart Homes According to GDPR Considering Cross-Border Issues. *Journal of Communications, 17*(3), 180-187.

Η ερευνητική εργασία υποστηρίχθηκε από το Ελληνικό Ίδρυμα Έρευνας και Καινοτομίας (ΕΛΙ.Δ.Ε.Κ.) στο πλαίσιο της Δράσης «Υποτροφίες ΕΛΙ.Δ.Ε.Κ. Υποψηφίων Διδακτόρων» (Αριθμός Υποτροφίας: 290)

[320] Hassan, Q. F. (Ed.). (2018). *Internet of things A to Z: technologies and applications*. John Wiley & Sons.

[321] King, N. (2003). Smart home–a definition. *Intertek Research and Testing Center*, pp. 1-6.

νοικοκυριού[322]. Ωστόσο, θα πρέπει να σημειωθεί ότι ο ορισμός των έξυπνων σπιτιών μπορεί να διαφοροποιείται ανάλογα με τις εκάστοτε τεχνολογίες που αξιοποιούνται σε αυτά[323]. Λαμβάνοντας υπόψη τις εφαρμογές των έξυπνων κατοικιών που αφορούν τον τομέα της παροχής υπηρεσιών, μία βασική κατηγοριοποίηση αναφέρεται στις υπηρεσίες κατ' οίκον φροντίδας, στον τομέα της άνεσης/ψυχαγωγίας, στον τομέα της ενέργειας και στις εφαρμογές ασφάλειας[324]. Ωστόσο, αυτή η κατηγοριοποίηση δε θα πρέπει να θεωρείται περιοριστική ή απόλυτη, καθώς οι δυνατότητες των έξυπνων σπιτιών είναι ένας αδιάκοπα αναπτυσσόμενος τομέας. Οι έξυπνες οικιακές συσκευές έχουν επεκταθεί ραγδαία στα μέλη των νοικοκυριών, και επομένως στα υποκείμενα των δεδομένων, ως καταναλωτικά προϊόντα[325]. Παράλληλα, οι καινοτομίες των έξυπνων σπιτιών, οι έξυπνες πόλεις και εν γένει τα τεχνολογικά επιτεύγματα του τομέα των επικοινωνιών, έχουν αναδείξει κινδύνους και περιορισμούς [326] [327]. Σύμφωνα με τους B. K. Sovacool και D. D. F. Del Rio[328], ο υψηλότερος αριθμός κινδύνων που σχετίζονται με τα έξυπνα σπίτια αποδίδεται, σύμφωνα με τις απόψεις εμπειρογνωμόνων, στους κινδύνους αναφορικά με την ιδιωτικότητα και την ασφάλεια. Σε ένα περιβάλλον έξυπνου σπιτιού, τα υποκείμενα των δεδομένων δύνανται να αποτελούνται από ενήλικες και ανηλίκους και, ως εκ τούτου, από άτομα με διαφορετικό επίπεδο ευαλωτότητας, όσον αφορά τα ζητήματα ιδιωτικότητας. Οι εφαρμογές των έξυπνων σπιτιών είναι δυνατό να συμβάλουν στη βελτίωση πολλών πτυχών της εκπαίδευσης, της θεραπείας και της ψυχαγωγίας των ανηλίκων[329]. Ωστόσο, σύμφωνα με τον GDPR, απαιτείται εξειδικευμένη προστασία των προσωπικών δεδομένων των παιδιών, καθώς

[322] Hassan, Q. F. (Ed.). (2018). *Internet of things A to Z: technologies and applications*. John Wiley & Sons.

[323] Bugeja, J. (2021). On privacy and security in smart connected homes.

[324] Bădică, C., Brezovan, M., & Bădică, A. (2013). An Overview of Smart Home Environments: Architectures, Technologies and Applications. *BCI*.

[325] Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-20.

[326] Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, *19*, 174-184.

[327] Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B. G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems*, *83*, 619-628.

[328] Sovacool, B. K., & Del Rio, D. D. F. (2020). Smart home technologies in Europe: a critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews*, *120*, 109663.

[329] Berrezueta-Guzman, J., Pau, I., Martín-Ruiz, M. L., & Máximo-Bocanegra, N. (2020). Smart-home environment to support homework activities for children. *IEEE Access*, *8*, 160251-160267.

ενδέχεται να μην έχουν γνώση των ζητημάτων ιδιωτικότητας [330] τα οποία συνοδεύουν τη χρήση μιας έξυπνης συσκευής. Το ευρωπαϊκό επίπεδο προστασίας των δεδομένων έχει διεθνή εμβέλεια για τις οντότητες, καθώς αυτή ισχύει για τα υποκείμενα των δεδομένων που βρίσκονται στην ΕΕ και τα υποκείμενα των δεδομένων που βρίσκονται εκτός της ΕΕ, όταν η επεξεργασία αναφέρεται στις λειτουργίες του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία εντός της ΕΕ, σύμφωνα με τις προϋποθέσεις του GDPR. Από τα προαναφερθέντα, συνάγεται το συμπέρασμα ότι οι οντότητες που βρίσκονται εκτός της ΕΕ (για παράδειγμα στις ΗΠΑ) θα πρέπει επίσης να λαμβάνουν υπόψη τις απαιτήσεις του GDPR, όπου απαιτείται σύμφωνα με το άρθρο 3 του Κανονισμού. Κατά συνέπεια, κρίνεται επιβεβλημένη η παρουσίαση του πλαισίου των διασυνοριακών ροών των προσωπικών δεδομένων. Το παρόν κεφάλαιο εξετάζει το εξειδικευμένο πλαίσιο διαφύλαξης της προστασίας των δεδομένων των ανηλίκων στο περιβάλλον των έξυπνων σπιτιών, με έμφαση στην προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό τους.

Το παρόν κεφάλαιο διαρθρώνεται ως εξής: εξετάζεται το πλαίσιο προστασίας των δεδομένων των ανηλίκων στα έξυπνα σπίτια με την παρουσίαση της τεχνικής της ανωνυμοποίησης, των μέτρων προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό, της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, των ζητημάτων γονικού ελέγχου, ανηλικότητας και συγκατάθεσης γονέα. Επίσης, εστιάζει στις επιπτώσεις της προστασίας των ανηλίκων στις διασυνοριακές ροές δεδομένων.

5.3 Το πλαίσιο της προστασίας των δεδομένων των ανηλίκων στα έξυπνα σπίτια

Εν πρώτοις, προκειμένου να αποσαφηνιστεί το πλαίσιο της προστασίας των δεδομένων των ανηλίκων εντός του έξυπνου οικιακού περιβάλλοντος, είναι απαραίτητη η εξειδίκευση των υποχρεώσεων που θεσπίζονται από τον GDPR και εφαρμόζονται από τα αρμόδια μέρη. Αρχικά, θα πρέπει να αναφερθεί ότι το προτεινόμενο πλαίσιο προστασίας των δεδομένων δεν αφορά αποκλειστικά τις συσκευές και τις υπηρεσίες, οι οποίες έχουν σχεδιαστεί για παιδιά, αλλά και όλες τις εφαρμογές των έξυπνων σπιτιών οι οποίες μπορούν να προσφερθούν σε ανηλίκους. Δεδομένου ότι ο υπεύθυνος της επεξεργασίας είναι το μέρος που

[330] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα, σελ. 17-30.

οφείλει να αποδεικνύει (άρθρο 5 παρ. 2 GDPR) τη συμμόρφωση με τις αρχές επεξεργασίας του Κανονισμού, ο υπεύθυνος επεξεργασίας έχει επίσης την ευθύνη για την εφαρμογή των κατάλληλων μέτρων για τη διατήρηση της προστασίας των δεδομένων των ανηλίκων στο πλαίσιο της χρήσης των συσκευών IoT στα έξυπνα σπίτια.

Όσον αφορά την εξαίρεση του νοικοκυριού στο άρθρο 2 παρ. 2 περ. γ του GDPR («Ο παρών κανονισμός δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:...από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,»), οι υπεύθυνοι επεξεργασίας δεδομένων στο πλαίσιο των έξυπνων σπιτιών τα επεξεργάζονται σε επαγγελματικό επίπεδο και όχι σε ιδιωτικό, αποκλείοντας την εν λόγω επεξεργασία από το να εμπίπτει στην εξαίρεση αυτή[331]. Στην πραγματικότητα, πρέπει να επισημανθεί ότι η εξαίρεση του άρθρου 2 παράγραφος 2 περ. γ του GDPR αναφέρεται στη δραστηριότητα που αφορά τον υπεύθυνο επεξεργασίας και, ως εκ τούτου, δεν αφορά τη δραστηριότητα των υποκειμένων των δεδομένων εντός των έξυπνων σπιτιών[332].

Τα ακόλουθα μέτρα και υποχρεώσεις, τα οποία θεσπίζονται από τον GDPR, αντιπροσωπεύουν τη συμμόρφωση με τον Κανονισμό, όταν η επεξεργασία[333] των δεδομένων αφορά παιδιά στο περιβάλλον των έξυπνων σπιτιών. Τα στοιχεία αυτά παρουσιάζονται στην Εικόνα 6, αναδεικνύοντας αφενός την επιμέρους σημασία τους και αφετέρου την αλληλεπίδρασή τους.

5.3.1 Ανωνυμοποίηση

Η πλήρης προστασία των δεδομένων, την οποία θα πρέπει να εφαρμόζει ο υπεύθυνος επεξεργασίας των δεδομένων, παρέχεται μέσω της ανωνυμοποίησης των προσωπικών δεδομένων. Οι υποχρεώσεις, τα δικαιώματα και οι αρχές του

[331] Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *Reconsidering Joint Controllership and the Household Exemption (November 18, 2019). International Data Privacy Law*.

[332] CJEU, *Judgment of the Court (Fourth Chamber) of 11 December 2014, in Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů*.

[333] «επεξεργασία»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή. (Άρθρο 4 περ. 2 GDPR)

GDPR δεν ισχύουν για ανώνυμα δεδομένα, τα οποία δεν σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (αιτιολογική σκέψη 26 GDPR). Σε αυτό το σημείο, κρίνεται απαραίτητη η αποσαφήνιση ότι οι έξυπνες οικιακές συσκευές του IoT περιβάλλονται από αναδυόμενες καινοτομίες, οι οποίες βασίζονται σε βασικές τεχνολογίες της βιομηχανίας. Ως αποτέλεσμα, η ανωνυμοποίηση θα πρέπει να επανεξετάζεται τακτικά σε σχέση με τα νέα στοιχεία κάθε επεξεργασίας εντός των εφαρμογών των έξυπνων σπιτιών, προκειμένου να παραμένει ένα αποτελεσματικό εργαλείο ασφαλείας των δεδομένων[334]. Εάν δεν επιτευχθεί η εφαρμογή της τεχνικής της ανωνυμοποίησης, θα πρέπει να εφαρμοστούν όλα τα ακόλουθα μέτρα (μέτρα προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό, εκτίμηση αντικτύπου, ζητήματα γονικού ελέγχου, ανηλικότητας και συγκατάθεσης γονέα).

5.3.2 Μέτρα προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό

Η προστασία των δεδομένων των παιδιών θα πρέπει να περιλαμβάνει τα ενισχυμένα μέτρα για την προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό, προκειμένου να προστατεύεται η συγκεκριμένη κατάστασή τους και να διασφαλίζεται η κατάλληλη γονική εποπτεία και γονικός έλεγχος.

Η συμμόρφωση με τον GDPR απαιτεί την επιβολή τεχνικών και οργανωτικών μέτρων σχετικά με μία συγκεκριμένη επεξεργασία δεδομένων (αιτιολογική σκέψη 78 GDPR).Τα εν λόγω κατάλληλα μέτρα συμπληρώνουν τις αρχές επεξεργασίας δεδομένων, τις υποχρεώσεις και τα δικαιώματα του GDPR (άρθρο 25 παρ. 1).

5.3.3 Εκτίμηση αντικτύπου για την προστασία των δεδομένων

Σε αυτό το σημείο, αναλύεται η υποχρέωση του υπεύθυνου επεξεργασίας να διενεργεί εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων (DPIA), πριν από την επεξεργασία των προσωπικών δεδομένων των ανηλίκων, μέσα σε ένα περιβάλλον έξυπνου σπιτιού. Η DPIA αποτελεί μία μέθοδο διαχείρισης που βασίζεται στην εκτίμηση των κινδύνων, αξιολογώντας τον κίνδυνο κάθε επεξεργασίας σε ένα συγκεκριμένο πλαίσιο. Η DPIA είναι υποχρεωτική σε περίπτωση που ενυπάρχει:

[334] Council of Europe, Consultative Committee of Convention 108. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01. Strasbourg. Διαθέσιμο στο: https://rm.coe.int/16806ebe7a

α) συστηματική και εκτενής αξιολόγηση των προσωπικών πτυχών,

β) ύπαρξη μεγάλης κλίμακας ευαίσθητων δεδομένων (άρθρο 9),

γ) δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα (άρθρο 10), ή

δ) συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα (άρθρο 35 παρ. 3 GDPR)[335].

Επιπλέον, έχουν υιοθετηθεί εννέα κριτήρια, προκειμένου να καθοριστεί η διεξαγωγή της DPIA και η κατάρτιση ειδικών καταλόγων από τα κράτη μέλη σε εθνικό επίπεδο[336]. Η ύπαρξη δύο ή περισσότερων κριτηρίων επιφέρει υψηλό κίνδυνο και απαιτεί τη διεξαγωγή της DPIA. Εν γένει, τα κριτήρια είναι: αξιολόγηση ή βαθμολόγηση βάσει προσωπικών δεδομένων, αυτοματοποιημένη λήψη αποφάσεων, συστηματική παρακολούθηση, ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα, δεδομένα μεγάλης κλίμακας επεξεργασίας, αντιστοίχιση ή συνδυασμός συνόλων δεδομένων, δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων, καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, και τέλος, η ύπαρξη επεξεργασίας που εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν δικαίωμα ή να χρησιμοποιήσουν υπηρεσία ή σύμβαση.

Πίνακας 2. Παράγοντες που οδηγούν στη διεξαγωγή της DPIA

Παράγοντες των έξυπνων σπιτιών που βασίζονται στο IoT σε σχέση με τα δεδομένα των ανηλίκων που οδηγούν στη διεξαγωγή της DPIA
Ευάλωτη κατάσταση των παιδιών
Συστηματική επεξεργασία μεγάλης κλίμακας δεδομένων
Αυτοματοποιημένη λήψη αποφάσεων
Το IoT θεωρείται μια καινοτόμος τεχνολογία με πιθανούς κινδύνους για την προστασία της ιδιωτικότητας

[335] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR interference with next generation 5G and IoT networks. *IEEE Access*, *8*, 108052-108061.

[336] Article 29 Working Party. (2018). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 250. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Στην περίπτωση επεξεργασίας προσωπικών δεδομένων ανηλίκων στο πλαίσιο των εφαρμογών των έξυπνων σπιτιών, όπως παρουσιάζεται στον ανωτέρω πίνακα, το πρώτο κριτήριο που συμβάλλει στη διεξαγωγή της DPIA είναι η ευάλωτη θέση των παιδιών ως υποκείμενα των δεδομένων. Τα παιδιά θεωρούνται μία ευαίσθητη κατηγορία υποκειμένων των δεδομένων λόγω της πιθανότητας υψηλότερων κινδύνων[337], δεδομένου ότι ενδέχεται να μην είναι σε θέση να κατανοήσουν και να διαχειριστούν τις αποφάσεις, οι οποίες καθορίζουν την προστασία των προσωπικών τους δεδομένων. Επιπλέον, όσον αφορά το είδος της επεξεργασίας σε σχέση με τη συγκεκριμένη τεχνολογία, οι έξυπνες οικιακές συσκευές του IoT δύνανται να περιλαμβάνουν συστηματική επεξεργασία μεγάλης κλίμακας δεδομένων και αυτοματοποιημένη λήψη αποφάσεων. Πιο συγκεκριμένα, οι συσκευές των έξυπνων σπιτιών είναι σε θέση να επεξεργάζονται αδιάκοπα μεγάλης κλίμακας δεδομένα λόγω των σκοπών που εξυπηρετούν, όπως η οικιακή ασφάλεια και η ρύθμιση της κατανάλωσης ενέργειας.

Η αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, για την οποία παρέχεται ειδική προστασία στο άρθρο 22 του GDPR[338] [339], συνδέεται κυρίως με την επεξεργασία δεδομένων των πτυχών του οικιακού βίου. Πιο συγκεκριμένα, οι οικιακές συσκευές μπορούν να αποκαλύψουν διαφορετικές πτυχές της προσωπικότητας των μελών του σπιτιού, αυξάνοντας τη δυνατότητα κατάρτισης προφίλ και στοχευμένης διαφήμισης[340]. Η απαραίτητη εξειδικευμένη προστασία των προσωπικών δεδομένων των ανηλίκων αφορά ιδίως «στη χρήση των δεδομένων προσωπικού χαρακτήρα με σκοπό την εμπορία ή τη δημιουργία προφίλ προσωπικότητας ή προφίλ χρήστη και τη συλλογή δεδομένων προσωπικού χαρακτήρα όσον αφορά παιδιά κατά τη χρήση υπηρεσιών που προσφέρονται άμεσα σε ένα παιδί» (αιτιολογική σκέψη 38 GDPR). Η επεξεργασία των προσωπικών δεδομένων των παιδιών, βάσει αυτοματοποιημένης λήψης αποφάσεων, επιτρέπεται μόνο με βάση τις εξαιρέσεις

[337] Article 29 Working Party. (2018). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 250. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[338] Milossi, M., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2021). AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach. *IEEE Access*, *9*, 58455-58466.

[339] Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, *24*(10), 1572-1593.

[340] Bugeja, J., & Jacobsson, A. (2019, August). On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces. In *IFIP International Summer School on Privacy and Identity Management* (pp. 126-141). Springer, Cham.

του άρθρου 22 παρ. 2 περ. α, β ή γ, μαζί με την προϋπόθεση η επεξεργασία να έχει στόχο την προστασία των δικαιωμάτων, των ελευθεριών και των νόμιμων συμφερόντων των παιδιών[341]. Επιπλέον, το IoT θεωρείται μία καινοτόμος τεχνολογία στο πλαίσιο της εκτίμησης αντίκτυπου[342].

Όλα τα προαναφερθέντα δεδομένα καταδεικνύουν τη σημασία της εκτίμησης αντίκτυπου για τους κινδύνους της ιδιωτικότητας. Όσον αφορά το αποτέλεσμα της DPIA, θα πρέπει να αναφερθεί ότι, εάν οι κίνδυνοι παραμένουν και μετά την εφαρμογή μέτρων για την προστασία της ιδιωτικότητας και της ασφάλειας των δεδομένων, ο υπεύθυνος της επεξεργασίας θα πρέπει να συμβουλεύεται την αρμόδια εποπτική αρχή[343].

5.3.4 Γονικός έλεγχος, ανηλικότητα και συγκατάθεση γονέα

Ένας ιδιαίτερα σημαντικός παράγοντας των εφαρμογών των έξυπνων σπιτιών, σε σχέση με τα παιδιά, είναι το ζήτημα του γονικού ελέγχου. Ο γονικός έλεγχος είναι το εργαλείο, το οποίο επιτρέπει στους γονείς ή τους κηδεμόνες να θέτουν συγκεκριμένους όρους σε σχέση με τη διαδικτυακή δραστηριότητα των ανηλίκων[344]. Αυτός θα μπορούσε να συμβάλει όχι μόνο στην ασφάλεια στον κυβερνοχώρο, αλλά και στη μείωση των κινδύνων της ιδιωτικότητας. Η πρακτική εφαρμογή της συγκατάθεσης του γονέα ή η γονική έγκριση της συγκατάθεσης του ανηλίκου εξαρτάται από το γεγονός ότι ο ανήλικος είναι ο χρήστης μιας συγκεκριμένης εφαρμογής. Συνεπώς, η αναγνώριση της ανηλικότητας αποτελεί την προϋπόθεση για όλα τα επόμενα βήματα της νόμιμης επεξεργασίας.

---

[341] Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[342] Article 29 Working Party. (2018). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 250. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[343] Article 29 Working Party. (2018). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 250. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[344] Information Commissioner's Office. (2020). "Age appropriate design: a code of practice for online services". Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

Το επόμενο στάδιο περιλαμβάνει τον προσδιορισμό της ηλικίας των ανηλίκων. Η αναγνώριση της ηλικίας ενός ανηλίκου διαδραματίζει καίριο ρόλο στη συγκατάθεση, η οποία θα μπορούσε να είναι η νομική βάση κάθε επεξεργασίας. Επιπροσθέτως, μια άλλη πτυχή της προστασίας των δεδομένων των ανηλίκων στα έξυπνα σπίτια είναι ο προσδιορισμός του φορέα της γονικής μέριμνας (άρθρο 8 παρ. 2). Η συγκατάθεση θα πρέπει να δοθεί, όχι από οποιονδήποτε ενήλικα που καθίσταται χρήστης του έξυπνου σπιτιού, αλλά από το πρόσωπο που έχει την επιμέλεια του ανηλίκου. Όσον αφορά τη συγκατάθεση ενός παιδιού, υπό τις προϋποθέσεις[345] του άρθρου 8 παρ. 1 του GDPR, υπάρχουν δύο περιπτώσεις με βάση την ηλικία του: α) 16 ετών και άνω και β) κάτω των 16 ετών.

Στην πρώτη περίπτωση, η συγκατάθεση του ανηλίκου 16 ετών και άνω είναι επαρκής, ενώ στη δεύτερη περίπτωση η συγκατάθεση του γονέα ή η γονική έγκριση της συγκατάθεσης του ανηλίκου είναι απαραίτητη[346]. Ωστόσο, τα κράτη-μέλη έχουν τη δυνατότητα να καθορίζουν, όπως και στην περίπτωση ευρωπαϊκής Οδηγίας, το κατάλληλο όριο ηλικίας για την υποχρεωτική συγκατάθεση ή έγκριση του γονέα, με γενικό όριο τα 13 έτη[347]. Αντιστοίχως, ο νόμος για την προστασία της ιδιωτικότητας των παιδιών στο διαδίκτυο (Children's Online Privacy Protection Rule, COPPA) των ΗΠΑ ορίζει το ίδιο όριο ηλικίας (13 ετών) για την προστασία των παιδιών. Πιο συγκεκριμένα, ο εν λόγω νόμος των ΗΠΑ απαιτεί, εν γένει, τη συγκατάθεση του γονέα με συγκεκριμένες εξαιρέσεις, πριν από τη ψηφιακή συλλογή προσωπικών δεδομένων από ανηλίκους κάτω των 13 ετών[348]. Αυτή η διάταξη του GDPR, αποδεικνύει ενεργά ότι οι υπεύθυνοι επεξεργασίας των δεδομένων και ιδίως οι προγραμματιστές των εφαρμογών θα πρέπει να αναγνωρίζουν και να επιβάλλουν το κατάλληλο όριο ηλικίας, σύμφωνα με τη συγκεκριμένη νομοθεσία της χώρας της ΕΕ, στην οποία βρίσκεται ο ανήλικος[349]. Θα πρέπει να αναφερθεί ότι, όταν δεν ισχύουν οι προϋποθέσεις του

[345] «…σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών απευθείας σε παιδί…». Βλ. Άρθρο 8 παρ. 1 GDPR

[346] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679. *ΔΙΜΕΕ, 1*, 5-19.

[347] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR interference with next generation 5G and IoT networks. *IEEE Access, 8*, 108052-108061.

[348] Federal Trade Commission. (2020). "Complying with COPPA: frequently asked questions." Διαθέσιμο στο: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

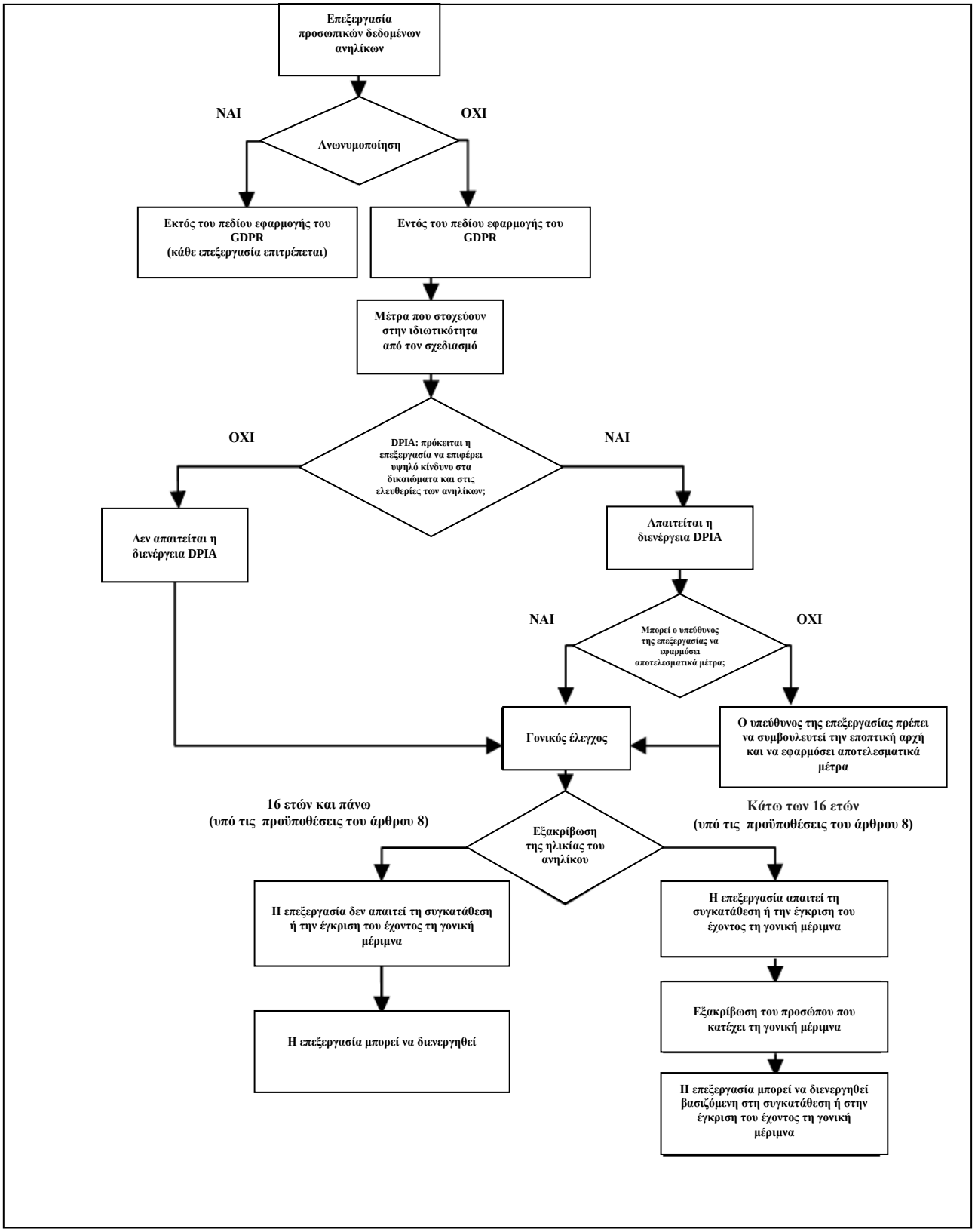
[349] Article 29 Working Party. (2013). Opinion 02/2013 on apps on smart devices. WP202. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/news-overview.cfm

άρθρου 8 παρ. 1 του GDPR, η συγκατάθεση του γονέα θα πρέπει να παρέχεται σύμφωνα με την εθνική νομοθεσία για την ανηλικότητα.

Όσον αφορά τα τεχνικά μέτρα, είναι απαραίτητο να αναφερθεί ότι έχει προταθεί[350] η συμβολή της τεχνητής νοημοσύνης στη διαδικασία αναγνώρισης της ηλικίας των ανηλίκων. Πιο συγκεκριμένα, στο περιβάλλον των έξυπνων σπιτιών, η συμπεριφορά και οι επιλογές του εκάστοτε χρήστη, ο οποίος σχετίζεται με πολλαπλούς και διαφορετικούς τύπους εφαρμογών, συνιστούν παράγοντες που μπορούν να υποδείξουν την ηλικία ενός ατόμου. Ως εκ τούτου, τα δεδομένα, τα οποία υποβάλλονται σε επεξεργασία μέσω έξυπνων σπιτιών, θα μπορούσαν να συμβάλουν στην προστασία των δεδομένων των παιδιών ως τεχνικό μέτρο. Ωστόσο, δεδομένου ότι η τεχνητή νοημοσύνη θα μπορούσε να συμπεριληφθεί στα μέτρα προστασίας των δεδομένων στα έξυπνα σπίτια, θα πρέπει να λαμβάνονται υπόψη οι περιπτώσεις της αιτιολογικής σκέψης 38 του GDPR[351], καθώς και η ανωνυμοποίηση αυτών των δεδομένων.

[350] Information Commissioner's Office. (2020). "Age appropriate design: a code of practice for online services". Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

[351] Σύμφωνα με την αιτιολογική σκέψη 38 του GDPR: «*…Αυτή η ειδική προστασία θα πρέπει να ισχύει ιδίως στη χρήση των δεδομένων προσωπικού χαρακτήρα με σκοπό την εμπορία ή τη δημιουργία προφίλ προσωπικότητας ή προφίλ χρήστη και τη συλλογή δεδομένων προσωπικού χαρακτήρα όσον αφορά παιδιά κατά τη χρήση υπηρεσιών που προσφέρονται άμεσα σε ένα παιδί…*»



Εικόνα 6. Η προστασία των δεδομένων των ανηλίκων στο έξυπνο οικιακό περιβάλλον μέσω του IoT

5.4 Πρακτική εφαρμογή και διασυνοριακά ζητήματα

Οι διασυνοριακές ροές δεδομένων[352] περιγράφονται ως οι «διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε αποδέκτες δικαιοδοσίας άλλου κράτους ή διεθνούς οργανισμού»[353]. Τρίτα κράτη, υπό το πρίσμα της ΕΕ, συνιστούν τα κράτη εκτός ΕΟΧ, ο οποίος περιλαμβάνει τις χώρες της ΕΕ, τη Νορβηγία, την Ισλανδία και το Λιχτενστάιν[354].

Όσον αφορά τη δραστηριότητα των ανηλίκων μέσω των έξυπνων οικιακών συσκευών, είναι απαραίτητο να αναλυθούν και οι διασυνοριακές προεκτάσεις του ζητήματος. Πιο συγκεκριμένα, η συλλογή και εν γένει η επεξεργασία των προσωπικών δεδομένων των ανηλίκων, στο περιβάλλον ενός έξυπνου σπιτιού που βασίζεται στο IoT, δύναται να περιέχει διασυνοριακές ροές δεδομένων. Συνεπώς, εάν μία θυγατρική εταιρεία που εδρεύει στον ΕΟΧ διαβιβάζει δεδομένα ανηλίκων στη μητρική της εταιρεία εκτός ΕΟΧ, τότε η διαβίβαση θα πρέπει να βασίζεται σε κάποιον μηχανισμό του GDPR για τις διεθνείς μεταφορές, παράλληλα με την εξασφάλιση εξειδικευμένης προστασίας για τους ανηλίκους, όπως παρουσιάζεται στην κατωτέρω εικόνα.

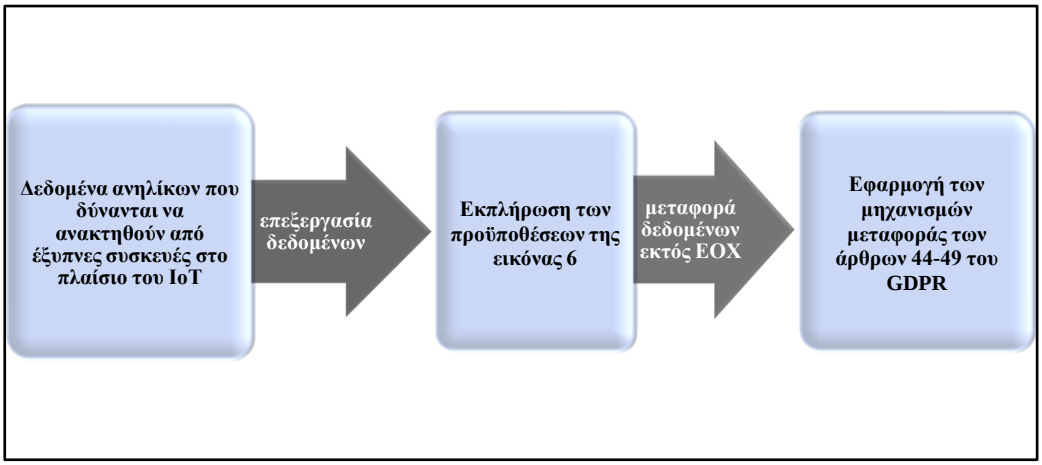
Εν πρώτοις, επιβάλλεται να αναφερθεί ότι οι διασυνοριακές ροές των δεδομένων καθορίζονται στα άρθρα 44-49 του GDPR. Οι διασυνοριακές ροές δεδομένων δύνανται να πραγματοποιούνται όταν υφίστανται: απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής, όσον αφορά την ισχύουσα νομοθεσία περί προστασίας των δεδομένων στην τρίτη χώρα (άρθρο 45)· κατάλληλες εγγυήσεις, όπως τυποποιημένες συμβατικές ρήτρες (standard data protection clauses, SCCs) και δεσμευτικοί εταιρικοί κανόνες (binding corporate rules, BCRs) που

[352] «διασυνοριακή επεξεργασία»: α) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων διάφορων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών επεξεργασία είναι εγκατεστημένος σε περισσότερα του ενός κράτη μέλη ή β) η επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία γίνεται στο πλαίσιο των δραστηριοτήτων μίας μόνης εγκατάστασης υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση αλλά που επηρεάζει ή ενδέχεται να επηρεάσει ουσιωδώς υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη. (Άρθρο 4 περ. 23 GDPR)

[353] Αιτιολογική Έκθεση του τροποποιητικού Πρωτοκόλλου της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ατόμων σε σχέση με την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (223/2018), στοιχείο 102.

[354] European Economic Area (EEA), "Relations with the EU". Διαθέσιμο στο: https://www.efta.int/eea

παρέχονται από τον υπεύθυνο επεξεργασίας δεδομένων (άρθρο 46)· παρεκκλίσεις (άρθρο 49), όπως η ρητή συγκατάθεση[355].



Εικόνα 7. Τα στάδια της προστασίας των προσωπικών δεδομένων των ανηλίκων

Είναι αξιοσημείωτη η παρουσίαση της προσέγγισης της ΕΕ μέσω πρόσφατων και επιλεγμένων αποφάσεων διαφορετικών εθνικών αρχών προστασίας δεδομένων της ΕΕ, προκειμένου να αναδειχθεί το διασυνοριακό πλαίσιο της προστασίας των δεδομένων των ανηλίκων.

5.4.1 Στοιχεία από τις Αρχές Προστασίας Δεδομένων της ΕΕ

Αρχικά, θα πρέπει να αναφερθεί η απόφαση της Νορβηγικής Αρχής Προστασίας Δεδομένων, η οποία έχει επιβάλει διοικητικό πρόστιμο ύψους 47.500 ευρώ σε Δήμο[356]. Αναλυτικότερα, στο πλαίσιο μίας πλατφόρμας ψηφιακής μάθησης,

[355] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

[356] Norwegian Data Protection Authority. (2020). "Final decision, administrative fine for Rælingen municipality,"Διαθέσιμο στο: https://www.datatilsynet.no/en/news/2020/final-decision-administrative-fine-for-ralingen-municipality/

υποβάλλονταν σε επεξεργασία προσωπικά δεδομένα παιδιών που αφορούσαν την υγεία. Μετά την κοινοποίηση της παραβίασης των εν λόγω δεδομένων από τον υπεύθυνο επεξεργασίας, η οποία είχε ως αποτέλεσμα την περαιτέρω έρευνα επί του ζητήματος, διαπιστώθηκε ότι το επίπεδο ασφάλειας της εφαρμογής δεν ήταν κατάλληλο σε συνάρτηση με τους κινδύνους που ενυπήρχαν. Τα βασικά στοιχεία της απόφασης αναφέρονται στην έλλειψη μίας ολοκληρωμένης εκτίμησης αντίκτυπου για την προστασία των δεδομένων (DPIA) πριν από τη διεξαγωγή οποιασδήποτε επεξεργασίας μέσω της συγκεκριμένης εφαρμογής. Η απόφαση κατέστησε σαφές ότι τα μέτρα ασφαλείας είναι απαραίτητα και θα πρέπει να είναι ανάλογα των κινδύνων που συνδέονται με την επεξεργασία των δεδομένων των ανηλίκων.

Επιπρόσθετα, θα πρέπει να σημειωθεί ότι η Σουηδική Αρχή Προστασίας των Δεδομένων επέβαλε διοικητικό πρόστιμο τεσσάρων εκατομμυρίων σουηδικής κορόνας (Swedish krona, SEK)[357], λόγω των αναποτελεσματικών μέτρων ασφάλειας των δεδομένων, όπως διαπιστώθηκε, σε ένα πληροφοριακό σύστημα που διαχειριζόταν προσωπικά δεδομένα ανηλίκων[358]. Η απόφαση υπογράμμισε ότι η συνεχής αξιολόγηση του επιπέδου προστασίας των δεδομένων είναι καίριας σημασίας στο πλαίσιο της επεξεργασίας μεγάλης κλίμακας δεδομένων.

Εκτός αυτού, η Ιταλική Αρχή Προστασίας Δεδομένων έλαβε πρόσφατα την απόφαση να περιορίσει την επεξεργασία των δεδομένων που ανήκουν σε υποκείμενα των οποίων η ηλικία δεν μπορούσε να εξακριβωθεί, στο πλαίσιο της λειτουργίας μίας επιγραμμικής εφαρμογής[359]. Ως εκ τούτου, γίνεται έκδηλη η διαπίστωση ότι η εξέταση της ηλικίας του ανηλίκου αποτελεί προϋπόθεση για τη νόμιμη επεξεργασία των προσωπικών δεδομένων των ανηλίκων, σύμφωνα με τη νομοθεσία της ΕΕ. Εκτός από το κύριο ζήτημα της υπόθεσης, θα πρέπει να αναφερθεί ότι η απόφαση επισημαίνει ότι η εφαρμογή προέβη πρόσφατα στην καταχώριση της κύριας εγκατάστασής της στην ΕΕ. Η εν λόγω μεταφορά της κύριας εγκατάστασης, θα μπορούσε να υποστηριχθεί ότι έχει ως αποτέλεσμα την

[357] European Central Bank, "Euro foreign exchange reference rates." Διαθέσιμο στο: https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/eurofxref-graph-sek.en.html

[358] Swedish Authority for Privacy Protection. (2020) "Serious deficiencies in the Stockholm online School Platform," Διαθέσιμο στο: https://www.imy.se/en/news/serious-deficiencies-in-the-stockholm-online-school-platform/

[359] Italian Data Protection Authority (Garante per la protezione dei dati personali). (2021). "Tik Tok: Italian SA imposes limitation on processing after the death of the girl from Palermo," Διαθέσιμο στο: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524224

εφαρμογή του GDPR και, ως εκ τούτου, την αποφυγή των διασυνοριακών περιορισμών. Παράλληλα, ο προσδιορισμός της ύπαρξης των διασυνοριακών ροών και των μηχανισμών τους επισημάνθηκε σε Πρακτικά της Ιταλικής Αρχής Προστασίας Δεδομένων που αφορούσαν τη δραστηριότητα ενός κοινωνικού δικτύου[360].

5.4.2 Οι μηχανισμοί διασυνοριακών ροών και η προστασία των δεδομένων των ανηλίκων

Καταρχάς, επιβάλλεται να αναφερθεί ότι ο πρωτεύων μηχανισμός των διασυνοριακών ροών δεδομένων είναι η απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής για την τρίτη χώρα, η οποία συνίσταται στην αξιολόγηση από την Ευρωπαϊκή Επιτροπή του επιπέδου προστασίας των δεδομένων στην τρίτη χώρα[361] [362] [363]. Η αξιολόγηση αυτή είναι εκτενής και θα πρέπει να περιέχει διάφορες πτυχές των υποχρεώσεων και των δικαιωμάτων του GDPR, συμπεριλαμβανομένων των διατάξεων για την προστασία των δεδομένων των ανηλίκων. Επί παραδείγματι, στην απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής για το Ηνωμένο Βασίλειο, ελέγχεται κατά πόσο το όριο ηλικίας για τη συγκατάθεση των ανηλίκων, δυνάμει του άρθρου 8, είναι συμβατό με τον GDPR[364]. Η εξέταση αυτού του ζητήματος, η οποία επιβεβαιώθηκε ότι εμπίπτει στα όρια του GDPR, αποδεικνύει ότι η αξιολόγηση στο πλαίσιο της έκδοσης απόφασης επάρκειας λαμβάνει υπόψη τα στοιχεία της νομοθεσίας των προσωπικών δεδομένων σχετικά με τους ανηλίκους.

---

[360] Italian Data Protection Authority (Garante per la protezione dei dati personali). (2020). "Tik Tok Endangers Children's Privacy: Italian Dpa Initiates Proceedings Against the Social Network," Διαθέσιμο στο: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923

[361] Council of Europe. (2018). *Handbook on European data protection law.* Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

[362] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων). *ΔΙΜΕΕ, 1*, 12-24.

[363] Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?. *International Data Privacy Law*, 8, 318–337.

[364] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf

Εάν δεν υφίσταται απόφαση επάρκειας για μία χώρα, η οποία πρόκειται να εισαγάγει προσωπικά δεδομένα, τότε ο υπεύθυνος της επεξεργασίας των δεδομένων θα πρέπει να καταφύγει στις κατάλληλες εγγυήσεις του άρθρου 46 του GDPR. Ο εν λόγω μηχανισμός μεταφοράς, ο οποίος περιλαμβάνει τα ειδικότερα εργαλεία του άρθρου, απαιτεί επιπλέον την αξιολόγηση της αποτελεσματικότητάς του, όσον αφορά όλες τις πτυχές της συγκεκριμένης μεταφοράς[365]. Ο μηχανισμός των κατάλληλων εγγυήσεων, στην περίπτωση των έξυπνων οικιακών συσκευών που βασίζονται στο IoT, οι οποίες χρησιμοποιούνται από ανηλίκους, θα πρέπει να αξιολογείται με βάση την προστασία των δεδομένων των ανηλίκων στην τρίτη χώρα. Εάν η νομοθεσία των προσωπικών δεδομένων των ανηλίκων είναι συμβατή με τη νομοθεσία της ΕΕ, μπορεί να αξιοποιηθεί το εργαλείο διαβίβασης του άρθρου 46. Σε αντίθετη περίπτωση, ο υπεύθυνος της επεξεργασίας θα πρέπει να λάβει περαιτέρω μέτρα, όπως η θέσπιση πολιτικών ασφαλείας[366].

Ειδικότερα, κατά την περίπτωση εφαρμογής του εργαλείου μεταφοράς των δεσμευτικών εταιρικών κανόνων (BCRs) του άρθρου 46, αυτό θα πρέπει να εγκριθεί από την αρμόδια εποπτική αρχή. Στο πλαίσιο διερεύνησης των στοιχείων της έγκρισης, είναι αναγκαίο να αναφερθεί ότι η προστασία των δεδομένων των παιδιών περιλαμβάνεται στον κατάλογο του προτεινόμενου εντύπου για τους δεσμευτικούς εταιρικούς κανόνες της ομάδας εργασίας του άρθρου 29[367]. Ως εκ τούτου, συνάγεται το συμπέρασμα ότι η μεταχείριση της προστασίας των δεδομένων των ανηλίκων μέσω των εφαρμογών των έξυπνων σπιτιών, στην περίπτωση των δεσμευτικών εταιρικών κανόνων, θα πρέπει να αντικατοπτρίζεται στο κείμενό τους.

Επιπλέον, εάν δεν υφίστανται ούτε αποφάσεις επάρκειας ούτε εγγυήσεις, η διαβίβαση δεδομένων θα πρέπει να βασίζεται στις παρεκκλίσεις του άρθρου

[365] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

[366] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_el

[367] Article 29 Data Protection Working Party. (2018). "Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data." WP264. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/recommendation-standard-application-form-approval-controller-binding_en

49[368] [369] [370]. Αξίζει να σημειωθεί ότι, ιδίως η προϋπόθεση του άρθρου 49 παρ. 1 περ. στ, που αναφέρεται στην περίπτωση κατά την οποία η διαβίβαση είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλων προσώπων (στην περίπτωση υποκειμένων των δεδομένων που είναι φυσικά ή νομικά ανίκανοι να παράσχουν τη συγκατάθεσή τους), δύναται να αφορά και τη δικαιοπρακτική ανικανότητα των ανηλίκων, η οποία καθορίζεται από την εκάστοτε εθνική νομοθεσία[371].

5.5 Συμπερασματικές παρατηρήσεις

Το παρόν κεφάλαιο αποσκοπεί στην αποσαφήνιση του πλαισίου της προστασίας των δεδομένων των ανηλίκων, σύμφωνα με τον GDPR. Για τον σκοπό αυτό λαμβάνονται υπόψη ο τεχνολογικός και νομικός τομέας μέσω της προσπάθειας υποστήριξης των ειδικών της τεχνολογίας των πληροφοριών και επικοινωνίας στον σχεδιασμό και στην εφαρμογή των διασφαλίσεων ιδιωτικότητας στις εφαρμογές έξυπνων σπιτιών, και ειδικότερα σε ό,τι αφορά την εξειδικευμένη προστασία των δεδομένων, η οποία είναι απαραίτητη για τους ανηλίκους. Παράλληλα, εξετάστηκαν οι διασυνοριακές προεκτάσεις του πλαισίου.

Πιο συγκεκριμένα, επιχειρήθηκε η διαλεύκανση των μέτρων προστασίας των δεδομένων με πρακτική εφαρμογή, τα οποία συνιστούν τις βασικές προκλήσεις της προστασίας των δεδομένων των ανηλίκων μέσω των έξυπνων κατοικιών. Παράλληλα, θα πρέπει να αναφερθεί ότι το πλαίσιο που παρουσιάστηκε, αναδεικνύει την προστασία της ιδιωτικότητας ήδη από τον σχεδιασμό, προκειμένου να συμβάλει στην ολιστική θεώρηση των δικαιωμάτων προστασίας των δεδομένων των ανηλίκων. Σε αυτήν την κατεύθυνση, μία πλευρά του πεδίου που δύναται να διερευνηθεί περαιτέρω αποτελεί η εξέταση των συγκεκριμένων μέτρων ασφαλείας από τον σχεδιασμό τα οποία θα μπορούσαν να διασφαλίσουν τον γονικό έλεγχο στο περιβάλλον του IoT.

---

[368] Ntouvas, I. (2019). Exporting personal data to EU-based international organizations under the GDPR. *International Data Privacy Law*, *9*(4), 272-284.

[369] Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, 485-532.

[370] Sullivan, C. (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. *computer law & security review*, *35*(4), 380-397.

[371] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_el

ΜΕΡΟΣ Β΄

ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΟΙΚΟΝΟΜΙΚΩΝ ΔΕΔΟΜΕΝΩΝ:

ΝΟΜΙΚΗ ΘΕΩΡΗΣΗ

ΚΕΦΑΛΑΙΟ 6. ΟΙ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΔΙΑΣΥΝΟΡΙΑΚΗΣ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΔΙΕΘΝΕΣ ΕΠΙΠΕΔΟ

6.1 Εισαγωγή

Τα διεθνή εργαλεία τα οποία περιλαμβάνουν τη θεσμοθέτηση των διασυνοριακών ροών των δεδομένων, παρότι δεν διαθέτουν ως επί το πλείστον δεσμευτικό χαρακτήρα[372], είναι σε θέση να επηρεάζουν τις εθνικές νομοθεσίες. Αναλυτικότερα, οι διεθνείς ρυθμίσεις αφενός καταδεικνύουν τις αρχές που διαπνέουν τον φορέα-οργανισμό τους σε σχέση με τη διασυνοριακή ροή των προσωπικών δεδομένων και αφετέρου αποτυπώνουν τη διαφορετική οπτική πάνω σε ένα ζήτημα που απαιτεί συγκρίσεις ως προς το επίπεδο προστασίας των δεδομένων.

Στην παρούσα ενότητα παρουσιάζονται τα σημαντικότερα διεθνή θεσμικά εργαλεία, όπως αποτυπώνονται στη διεθνή βιβλιογραφία[373] [374] [375] [376], τα οποία περιλαμβάνουν διατάξεις για τη διασυνοριακή ροή των δεδομένων. Θα πρέπει να αναφερθεί ότι τα επιλεγμένα διεθνή κείμενα καλύπτουν ένα ευρύ γεωγραφικό φάσμα, πλην των αμιγώς ευρωπαϊκών ρυθμίσεων, οι οποίες αναλύονται στο κεφάλαιο 8. Η καταγραφή των διεθνών κειμένων στο παρόν πόνημα γίνεται από το παλαιότερο στο νεότερο με στόχο τη διαχρονική παρακολούθηση της εξέλιξης του ζητήματος της διασυνοριακής ροής των δεδομένων σε διεθνές επίπεδο.

6.2 Οι κατευθυντήριες γραμμές του ΟΟΣΑ από το 1980 για την προστασία της ιδιωτικής ζωής και τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα

Η πρώτη διεθνής ρύθμιση της διασυνοριακής ροής δεδομένων είναι «*Οι κατευθυντήριες γραμμές του ΟΟΣΑ*[377] *για την προστασία της ιδιωτικής ζωής και τη*

[372] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p. 25-26.

[373] Casalini, F., & González, J. L. (2019). Trade and cross-border data flows.

[374] Spiezia, V. (2020). International agreements on cross-border data flows and international trade: A statistical analysis.

[375] Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford.

[376] OECD/IDB (2016). Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit. Διαθέσιμο στο: http://dx.doi.org/10.1787/9789264251823-en

[377] Για τα μέλη του ΟΟΣΑ Βλ. https://www.oecd.org/about/document/ratification-oecd-convention.htm

διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα»[378] της 23ης Σεπτεμβρίου 1980[379]. Μετά την υιοθέτηση των πρώτων νομοθετικών πρωτοβουλιών για την προστασία της ιδιωτικότητας από τη δεκαετία του 1970, ο ΟΟΣΑ το έτος 1978 ανέθεσε σε μια ομάδα εμπειρογνωμόνων τη σύνταξη των κατευθυντήριων γραμμών, προκειμένου, όπως αναφέρεται στην αιτιολογική έκθεσή τους, να συμβάλουν στην εναρμόνιση των εθνικών νομοθεσιών στο ζήτημα της προστασίας της ιδιωτικότητας και της διασυνοριακής ροής των δεδομένων[380]. Πιο συγκεκριμένα, θα μπορούσε να αναφερθεί ότι αποτέλεσαν την πρώτη προσπάθεια γεφύρωσης της διαφορετικής οπτικής στο ζήτημα της προστασίας της ιδιωτικότητας ανάμεσα στις ΗΠΑ και στην ΕΕ, ώστε να αποφευχθούν νομικά και οικονομικά εμπόδια στη διεθνή διακίνηση των δεδομένων [381].

Καταρχάς θα πρέπει να σημειωθεί ότι οι κατευθυντήριες γραμμές αποτελούν μία μη δεσμευτική ρύθμιση με συμπληρωματικό ρόλο (παρ. 6 του πρώτου μέρους του Παραρτήματος) στη θέσπιση νόμων για την προστασία της ιδιωτικότητας[382] [383]. Προκειμένου να αναλυθούν οι διατάξεις των κατευθυντήριων γραμμών που αφορούν τις διασυνοριακές ροές των δεδομένων, αξίζει να γίνει αναφορά στο πλαίσιο που τις καθόρισε. Πιο συγκεκριμένα, κατά το χρονικό σημείο σύνταξης των κατευθυντήριων γραμμών του ΟΟΣΑ, οι διασυνοριακές ροές των δεδομένων αποτελούσαν, ως επί το πλείστον, συγκεκριμένες και διακριτές μεταφορές δεδομένων από σημείο σε σημείο στα πλαίσια λειτουργίας των επιχειρήσεων ή των κρατών[384].

---

[378] Βλ. OECD (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[379] Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, No. 187. OECD Publishing.

[380] Βλ. OECD (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[381] Kirby, M. (2011). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law*, *1*(1), 6-14.

[382] Βλ. OECD (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[383] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p. 35.

[384] OECD.(2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

Εν γένει, οι κατευθυντήριες γραμμές ανέδειξαν την ανάγκη αυτοτελούς θεσμοθέτησης των διασυνοριακών ροών των δεδομένων[385]. Αναλυτικότερα, η αποτύπωση της σημαντικής θέσης που αποδίδεται στις διασυνοριακές ροές δεδομένων αντανακλάται και στον τίτλο της ρύθμισης. Επιπλέον, το τρίτο μέρος των κατευθυντήριων γραμμών αφιερώνεται στη διασυνοριακή ροή των δεδομένων με τίτλο: «*Βασικές αρχές της διεθνούς εφαρμογής: ελεύθερη ροή και νομοθετικοί περιορισμοί*», αναδεικνύοντας τον κεντρικό άξονα της ρύθμισης, ο οποίος έγκειται στην αποφυγή των διασυνοριακών περιορισμών. Οι διατάξεις των παραγράφων 15 έως 18 περιλαμβάνουν τη διασυνοριακή ροή δεδομένων.

Οι κατευθυντήριες γραμμές του 1980 εκκίνησαν από το γεγονός ότι οι διασυνοριακές ροές δεδομένων πρέπει εν γένει να επιτρέπονται (παρ. 16). Ωστόσο, αναγνωρίζεται στην παρ. 17 η δυνατότητα των κρατών να περιορίζουν, υπό ορισμένες περιστάσεις, τη διασυνοριακή ροή των προσωπικών δεδομένων[386]. Πιο συγκεκριμένα, οι περιορισμοί επιτρέπονται, σύμφωνα με τις κατευθυντήριες γραμμές, όταν η χώρα εισαγωγής δε λαμβάνει υπόψη τις κατευθυντήριες γραμμές του ΟΟΣΑ και όταν γίνεται εξαγωγή εκ νέου των δεδομένων, η οποία αντιβαίνει στην εθνική νομοθεσία περί προστασίας της ιδιωτικότητας.

Παράλληλα, θα πρέπει να αναφερθεί ότι οι κατευθυντήριες γραμμές εισάγουν για πρώτη φορά την αρχή της λογοδοσίας στο πλαίσιο της προστασίας της ιδιωτικότητας[387]. Ειδικότερα, η παρ. 14 αναφέρεται στην υποχρέωση του υπεύθυνου της επεξεργασίας των δεδομένων να συμμορφώνεται με τις διατάξεις των κατευθυντήριων γραμμών.

Στο σημείο αυτό, θα γίνει αναφορά της αναθεώρησης[388] του 2013 και σύγκριση με τις κατευθυντήριες γραμμές του 1980. Η αναθεώρηση του 2013 είναι η πρώτη από την αρχική εκδοχή των κατευθυντήριων γραμμών του 1980. Στην αναθεωρημένη έκδοση των κατευθυντήριων γραμμών, η θεσμοθέτηση της προστασίας της διασυνοριακής ροής των δεδομένων περιλαμβάνεται στο τέταρτο μέρος, υπό τον ίδιο τίτλο, καταλαμβάνοντας τις παραγράφους 16 έως 18. Αρχικά,

[385] Kirby, M. (2011). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law*, *1*(1), 6-14.

[386] OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

[387] Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, No. 187. OECD Publishing.

[388] Βλ. OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

θα πρέπει να επισημανθεί μία ιδιαίτερα σημαντική διαφοροποίηση της αναθεωρημένης εκδοχής, η οποία αφορά την αρχή της λογοδοσίας.

Αναλυτικότερα, η παρ. 16 μεταφέρει την αρχή της λογοδοσίας στο πεδίο της διασυνοριακής ροής των δεδομένων, καθιστώντας τον εξαγωγέα των δεδομένων υπεύθυνο/υπόλογο για την προστασία των δεδομένων, ανεξάρτητα της τοποθεσίας τους. Η διάταξη αυτή στοχεύει στην εξασφάλιση της προστασίας των διαβιβαζόμενων δεδομένων ανεξαρτήτως της χώρας εισαγωγής. Συνεπώς, θα πρέπει να επισημανθεί πως η προσέγγιση αυτή του ΟΟΣΑ έρχεται σε άμεση αντιστοιχία με την προσέγγιση της διασυνοριακής ροής δεδομένων με κριτήριο τους οργανισμούς (στην οποία γίνεται ανάλυση στο κεφάλαιο 1) και την υποχρέωση λογοδοσίας, σε αντίθεση με το ευρωπαϊκό μοντέλο σύγκρισης των επιπέδων προστασίας των δεδομένων με κριτήριο την τοποθεσία και την εξωεδαφική εμβέλεια (στο οποίο γίνεται ανάλυση στο κεφάλαιο 1).

Εν συνεχεία, η παρ. 17, σε σχέση με την αρχική εκδοχή του 1980, τοποθετεί τους εν δυνάμει περιορισμούς στη διασυνοριακή ροή δεδομένων από το πλαίσιο των εξαιρέσεων των περιπτώσεων (α) και (β) σε ένα πλαίσιο θεμιτών συμπεριφορών στις οποίες θα πρέπει να αποφεύγονται οι περιορισμοί. Πιο συγκεκριμένα, η αναθεωρημένη εκδοχή των κατευθυντηρίων γραμμών του 2013, διατηρεί στην περίπτωση (α) την αποφυγή των περιορισμών της διασυνοριακής ροής δεδομένων, όταν η χώρα εξαγωγής λαμβάνει υπόψη τις κατευθυντήριες γραμμές. Εντούτοις, θα πρέπει να αναφερθεί ότι η περ. (β) της παρ. 17 τροποποιήθηκε ριζικά. Ειδικότερα, τα κράτη θα πρέπει να απέχουν από την επιβολή περιορισμών όταν: «υφίστανται επαρκείς διασφαλίσεις, συμπεριλαμβανομένων αποτελεσματικών μηχανισμών επιβολής και κατάλληλων μέτρων από τον υπεύθυνο επεξεργασίας των δεδομένων, ώστε να διασφαλίζεται η ύπαρξη ενός συνεχούς επιπέδου προστασίας σύμφωνα με αυτές τις κατευθυντήριες γραμμές». Επομένως, η παρ. 17 περ. (β) εισάγει την επιβολή αποτελεσματικών μέτρων, τα οποία σύμφωνα με τη συμπληρωματική αιτιολογική έκθεση των αναθεωρημένων κατευθυντήριων γραμμών[389], μπορεί να συνίστανται σε μέτρα διοικητικής και δικαστικής εποπτείας, καθώς και σε μέτρα διασυνοριακής συνεργασίας μεταξύ των εποπτικών αρχών προστασίας των προσωπικών δεδομένων.

Παράλληλα, η παρ. 18, όπως ισχύει, εστιάζει περισσότερο στην αρχή της αναλογικότητας, η οποία θα πρέπει να διέπει τους περιορισμούς της διασυνοριακής ροής των δεδομένων. Ειδικότερα, ενώ η αρχική διάταξη του 1980

[389] OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

αναφέρεται σε αποφυγή εμποδίων στη διασυνοριακή ροή δεδομένων, τα οποία θα υπερβαίνουν τις απαιτήσεις της προστασίας των προσωπικών δεδομένων, η αναθεωρημένη διάταξη αναφέρεται σε «περιορισμούς ανάλογους με τους κινδύνους που παρουσιάζονται». Καθίσταται σαφές, λοιπόν, ότι εισάγεται μία διαδικασία στάθμισης των κινδύνων, η οποία έρχεται σε αντιστοιχία με την προσέγγιση βασισμένη στον κίνδυνο, η οποία διαπνέει τις κατευθυντήριες γραμμές[390].

Όσον αφορά την παράγραφο 6 των «*Γενικών Ορισμών*» στο πρώτο μέρος, στην αναθεώρηση του 2013 προστέθηκε η αναφορά της διασυνοριακής ροής δεδομένων στους λόγους θέσπισης συμπληρωματικών πρόσθετων μέτρων από τα κράτη, ενώ στην αρχική εκδοχή γινόταν αναφορά μόνο στην προστασία της ιδιωτικής ζωής και των ατομικών ελευθεριών. Κατά συνέπεια, συμπεραίνεται ότι εν συνόλω η αναθεώρηση του 2013 αναβάθμισε τη σημασία των διασυνοριακών ροών των δεδομένων, οριοθετώντας το πλαίσιο περιορισμών τους και εστιάζοντας στην αξία τους, η οποία ενισχύεται με την ανάπτυξη των νέων τεχνολογιών.

6.3 Η σύμβαση 108/1981 του Συμβουλίου της Ευρώπης και το πρόσθετο πρωτόκολλο 181/2001

Η Σύμβαση 108/1981[391] του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, η οποία άνοιξε για υπογραφή στις 28 Ιανουαρίου 1981, αποτέλεσε την πρώτη νομικά δεσμευτική διεθνή ρύθμιση στο πεδίο της προστασίας των προσωπικών δεδομένων[392]. Στο παρόν πόνημα, η Σύμβαση 108/1981 περιλαμβάνεται στο παρόν κεφάλαιο λόγω της διευρυμένης εμβέλειάς της, η οποία εκτείνεται και σε μέλη[393] εκτός της ΕΕ. Ως προς το εύρος εφαρμογής και

[390] Βλ. OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

[391] Συμβούλιο της Ευρώπης. Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, CETS αριθ. 108, 1981.

[392] Βλ. https://www.coe.int/en/web/data-protection/convention108/background

[393] Τα μέλη του Συμβουλίου της Ευρώπης αποτελούνται αλφαβητικά από τα εξής κράτη: Αζερμπαϊτζάν, Αλβανία, Ανδόρα, Αρμενία, Αυστρία, Βέλγιο, Βοσνία Ερζεγοβίνη, Βουλγαρία, Βόρεια Μακεδονία, Γαλλία, Γερμανία, Γεωργία, Δανία, Ελβετία, Ελλάδα, Εσθονία, Ηνωμένο Βασίλειο, Ιρλανδία, Ισλανδία, Ισπανία, Ιταλία, Κροατία, Κύπρος, Λετονία, Λιθουανία, Λιχτενστάιν, Λουξεμβούργο, Μάλτα, Μαυροβούνιο, Μολδαβία, Μονακό, Νορβηγία, Ολλανδία, Ουγγαρία, Ουκρανία, Πολωνία, Πορτογαλία, Ρουμανία, Ρωσική Ομοσπονδία, Σαν Μαρίνο, Σερβία, Σλοβακική Δημοκρατία, Σλοβενία, Σουηδία, Τουρκία, Τσεχική Δημοκρατία, Φινλανδία.

δεσμευτικότητάς της, θα πρέπει να αναφερθεί ότι, σύμφωνα με την παρ. 38 της Αιτιολογικής Έκθεσης[394] της Σύμβασης, δεν μπορεί να αποτελέσει τη βάση διεκδίκησης δικαιωμάτων από ιδιώτες, αλλά υποχρεώνει τα μέρη να την ενσωματώσουν στην εθνική τους νομοθεσία για την προστασία των προσωπικών δεδομένων.

Εν συνεχεία, εκδόθηκε το πρόσθετο πρωτόκολλο 181/2001[395] στη Σύμβαση 108, το οποίο εισήγαγε διατάξεις σχετικά με τη διασυνοριακή ροή δεδομένων σε μη συμβαλλόμενα μέρη (δηλαδή τρίτες χώρες) και με την υποχρέωση σύστασης εθνικών εποπτικών αρχών προστασίας των προσωπικών δεδομένων[396]. Ειδικότερα, στο πεδίο της διασυνοριακής ροής δεδομένων, το πρόσθετο πρωτόκολλο 181/2001 έθεσε στο άρθρο 2 τις προϋποθέσεις της μεταφοράς δεδομένων σε τρίτες χώρες, οι οποίες έγκεινται στο επαρκές επίπεδο προστασίας της τρίτης χώρας και σε παρεκκλίσεις (συμφέροντα του υποκειμένου, έννομα συμφέροντα, δημόσιο συμφέρον, εγγυήσεις). Συνεπώς, καθίσταται έκδηλη η πρόθεση ευθυγράμμισης των παραπάνω ρυθμίσεων με την Οδηγία 95/46/ΕΚ. Θα πρέπει να αναφερθεί ότι το πρόσθετο πρωτόκολλο 181/2001 δεν εφαρμόζεται πλέον, καθώς οι διατάξεις του επικαιροποιήθηκαν και ενσωματώθηκαν στην Εκσυγχρονισμένη Σύμβαση 108[397].

Το ισχύον τροποποιητικό πρωτόκολλο[398] της Εκσυγχρονισμένης Σύμβασης εγκρίθηκε στις 18 Μαΐου 2018[399]. Επί του παρόντος τα συμβαλλόμενα μέρη στη Σύμβαση 108 είναι όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης (47 χώρες) και επιπροσθέτως τα εξής κράτη: Αργεντινή, Cabo Verde (Πράσινο Ακρωτήρι), Μαρόκο, Μαυρίκιος, Μεξικό, Ουρουγουάη, Σενεγάλη και

[394] Συμβούλιο της Ευρώπης. Αιτιολογική Έκθεση της Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, Στρασβούργο, 28.1.1981.

[395] Συμβούλιο της Ευρώπης. Πρόσθετο Πρωτόκολλο στη Σύμβαση για την προστασία των προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχετικά με τις εποπτικές αρχές και τη διασυνοριακή ροή δεδομένων, CETS αριθ. 181, 2001.

[396] Συμβούλιο της Ευρώπης. (2018). *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης.

[397] Συμβούλιο της Ευρώπης. (2018). *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης.

[398] Συμβούλιο της Ευρώπης. Εκσυγχρονισμένη Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, CETS αριθ. 223, 2018.

[399] Βλ. https://www.coe.int/en/web/data-protection/convention108/background

Τυνησία[400]. Ο εκσυγχρονισμός της Σύμβασης 108 επιδίωξε δύο βασικούς στόχους: αφενός την αντιμετώπιση των προκλήσεων που απορρέουν από τη χρήση των νέων τεχνολογιών των πληροφοριών και των επικοινωνιών και αφετέρου την ενίσχυση της αποτελεσματικής εφαρμογής της Σύμβασης[401].

Στο παρόν σημείο γίνεται αναφορά στο διαχρονικό πλαίσιο των διασυνοριακών ροών των προσωπικών δεδομένων. Ειδικότερα, θα παρατεθεί το ισχύον καθεστώς των διασυνοριακών ρυθμίσεων του Συμβουλίου της Ευρώπης με αναφορά στα προϊσχύοντα ερείσματά του. Καταρχάς, θα πρέπει να αναφερθεί ότι η ρύθμιση των διασυνοριακών ροών των προσωπικών δεδομένων αντιμετωπίζεται στο άρθρο 14 της Εκσυγχρονισμένης Σύμβασης 108. Επιπλέον, είναι σημαντικό να επισημανθεί η εν όλω κατάργηση του άρθρου 2 του πρόσθετου πρωτοκόλλου 181/2001. Πιο συγκεκριμένα, το περιεχόμενο του καταργηθέντος άρθρου 2, στο οποίο αναφέρονταν οι μηχανισμοί της διασυνοριακής ροής των δεδομένων βάσει του δικαίου του Συμβουλίου της Ευρώπης, στην Εκσυγχρονισμένη Σύμβαση 108 έχει πλέον μεταφερθεί στο άρθρο 14. Αναλυτικότερα, οι διασυνοριακές ροές των δεδομένων, εισαγόμενες σε κράτος το οποίο δεν αποτελεί συμβαλλόμενο μέρος, επιτρέπονται μόνον εάν υπάρχει κατάλληλο επίπεδο προστασίας[402].

Επιπλέον, σύμφωνα με την παρ. 3 του άρθρου 14 περ. a, οι ελεύθερες διαβιβάσεις δεδομένων προς μη συμβαλλόμενα μέρη της Σύμβασης επιτρέπονται μόνο με βάση: «το δίκαιο του κράτους ή του διεθνούς οργανισμού, συμπεριλαμβανομένων των εφαρμοστέων διεθνών συνθηκών ή συμφωνιών που διασφαλίζουν κατάλληλες εγγυήσεις, ειδικές ή εγκεκριμένες τυποποιημένες εγγυήσεις που παρέχονται από νομικώς δεσμευτικά και εκτελεστά μέσα τα οποία θεσπίζονται και εφαρμόζονται από τα πρόσωπα που συμμετέχουν στη διαβίβαση και την περαιτέρω επεξεργασία». Η παρ. 3 του άρθρου 14 δεν εισάγει κάποιο νέο εργαλείο για τη διασυνοριακή ροή των δεδομένων.

Οι παρεκκλίσεις της παρ. 4 του άρθρου 14 επιτρέπονται μόνο σε περίπτωση: «*συγκατάθεσης ή συγκεκριμένου συμφέροντος του υποκειμένου των δεδομένων ή/και όταν υπάρχουν έννομα συμφέροντα ή/και η μεταφορά αποτελεί απαραίτητο και αναλογικό μέτρο σε μία δημοκρατική κοινωνία για την ελευθερία της έκφρασης*»[403]. Οι δύο ουσιαστικές διαφοροποιήσεις του ισχύοντος άρθρου 14

[400]Βλ.https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

[401]Βλ. για την Εκσυγχρονισμένη Σύμβαση 108 (Modernisation of Convention 108): https://www.coe.int/en/web/data-protection/convention108/modernised

[402] Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 2.

[403] Βλ. Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, άρθρο 113.

έγκεινται στην εισαγωγή στο δίκαιο του Συμβουλίου της Ευρώπης των περ. a και d της παρ. 4 του άρθρου 14 της Εκσυγχρονισμένης Σύμβασης 108. Οι δύο νέοι μηχανισμοί της διασυνοριακής ροής των δεδομένων ανήκουν στο πεδίο των παρεκκλίσεων/εξαιρέσεων όταν οι χώρες εισαγωγής δεν εξασφαλίζουν επαρκή προστασία των προσωπικών δεδομένων[404]. Όσον αφορά την περ. a της παρ. 4 του άρθρου 14, αυτή περιλαμβάνει τη ρητή συγκατάθεση του υποκειμένου των δεδομένων, σε αντιστοιχία με την προϊσχύουσα Οδηγία 95/46/ΕΚ, αλλά και τον ισχύοντα GDPR. Η περ. d της παρ. 4 του άρθρου 14 εισάγει την εξαίρεση της μεταφοράς των δεδομένων όταν πρόκειται για αναγκαίο και αναλογικό μέτρο σε μία δημοκρατική κοινωνία.

Επιπροσθέτως, όσον αφορά το δίκαιο της ΕΕ για τη διασυνοριακή ροή των δεδομένων, η παρ. 108 της Αιτιολογικής Έκθεσης της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται στη σχέση της με τον GDPR στο πεδίο της χορήγησης απόφασης επάρκειας από την Ευρωπαϊκή Επιτροπή. Ειδικότερα, επισημαίνεται ότι η προσχώρηση τρίτης χώρας στη Σύμβαση 108 αποτελεί σημαντικό παράγοντα στην αξιολόγηση της τρίτης χώρας ως προς το επαρκές επίπεδο προστασίας. Η ίδια συσχέτιση της Εκσυγχρονισμένης Σύμβασης 108 και του GDPR στο θέμα της επάρκειας των τρίτων χωρών αναφέρεται και στην αιτιολογική σκέψη 105 του Κανονισμού.

6.4 Οι κατευθυντήριες γραμμές προστασίας προσωπικών δεδομένων σε αυτοματοποιημένα αρχεία της Γενικής Συνέλευσης των Ηνωμένων Εθνών

Οι κατευθυντήριες γραμμές της προστασίας των προσωπικών δεδομένων σε αυτοματοποιημένα αρχεία[405], οι οποίες εγκρίθηκαν με το ψήφισμα 45/95 της Γενικής Συνέλευσης της 14ης Δεκεμβρίου 1990, αποτελούν ένα μη νομικά δεσμευτικό (για φυσικά πρόσωπα, νομικά πρόσωπα ή χώρες) διεθνές εργαλείο[406].

Η ρύθμιση των διασυνοριακών ροών των προσωπικών δεδομένων καταλαμβάνει το άρθρο 9, υπό τον αντίστοιχο τίτλο (διασυνοριακές ροές δεδομένων). Αναλυτικότερα, «*όταν η νομοθεσία δύο ή περισσοτέρων χωρών που αφορά μια διασυνοριακή ροή δεδομένων θεσπίζει αντίστοιχες διασφαλίσεις για την προστασία της ιδιωτικής ζωής, τα δεδομένα θα πρέπει να κυκλοφορούν όσο*

[404]Βλ. Συμβούλιο της Ευρώπης. (2018). *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης.

[405]United Nations. (1990). The guidelines concerning computerized personal data files.

[406]Βλ. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/un-guidelines

ελεύθερα κυκλοφορούν και εντός του κράτους. Εάν δεν υπάρχουν αμοιβαίες διασφαλίσεις, οι περιορισμοί στην κυκλοφορία αυτή δε θα πρέπει να επιβάλλονται αδικαιολόγητα και θα πρέπει να υποβάλλονται μόνο στο βαθμό που είναι αναγκαίο για την προστασία της ιδιωτικής ζωής».

Αρχικά, θα πρέπει να αναφερθεί ότι, μέσω της διατύπωσης του άρθρου 9, διαφαίνεται μία γενική προσέγγιση στο ζήτημα των διασυνοριακών ροών των προσωπικών δεδομένων. Πιο συγκεκριμένα, δε γίνεται αναφορά σε συγκεκριμένους μηχανισμούς για τη διασυνοριακή ροή των δεδομένων, ούτε τίθεται ένα συγκεκριμένο επιβαλλόμενο επίπεδο προστασίας των δεδομένων, το οποίο να οριοθετείται από τις ίδιες τις Κατευθυντήριες γραμμές, όπως στην περίπτωση του ΟΟΣΑ. Κινούμενο σε ένα διευρυμένο θεσμικό πλαίσιο, το άρθρο 9 των κατευθυντηρίων γραμμών των Ηνωμένων Εθνών εισάγει την έννοια της αναγκαιότητας της επιβολής περιορισμών στις διασυνοριακές ροές των δεδομένων. Η έκφανση αυτή της αρχής της αναλογικότητας αναφέρεται στη στάθμιση αφενός της καταλληλότητας και αφετέρου της αναγκαιότητας των περιορισμών των διασυνοριακών ροών χάριν της προστασίας των προσωπικών δεδομένων.

6.5 Η Σύσταση R (99) 5 της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης

Στο παρόν πόνημα, η Σύσταση R (99) 5[407] περιλαμβάνεται στο παρόν κεφάλαιο λόγω της διευρυμένης εμβέλειάς της, η οποία εκτείνεται και σε μέλη[408] εκτός της ΕΕ. Η Σύσταση R (99) 5 αποτελείται από κατευθυντήριες γραμμές, χωρίς νομική δεσμευτικότητα[409].

[407] Committee of Ministers of the Council of Europe. (1999). Σύσταση R (99) 5 on the protection of privacy on the Internet. Διαθέσιμο στο: https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

[408] Τα μέλη του Συμβουλίου της Ευρώπης αποτελούνται αλφαβητικά από τα εξής κράτη: Αζερμπαϊτζάν, Αλβανία, Ανδόρα, Αρμενία, Αυστρία, Βέλγιο, Βοσνία Ερζεγοβίνη, Βουλγαρία, Βόρεια Μακεδονία, Γαλλία, Γερμανία, Γεωργία, Δανία, Ελβετία, Ελλάδα, Εσθονία, Ηνωμένο Βασίλειο, Ιρλανδία, Ισλανδία, Ισπανία, Ιταλία, Κροατία, Κύπρος, Λετονία, Λιθουανία, Λιχτενστάιν, Λουξεμβούργο, Μάλτα, Μαυροβούνιο, Μολδαβία, Μονακό, Νορβηγία, Ολλανδία, Ουγγαρία, Ουκρανία, Πολωνία, Πορτογαλία, Ρουμανία, Ρωσική Ομοσπονδία, Σαν Μαρίνο, Σερβία, Σλοβακική Δημοκρατία, Σλοβενία, Σουηδία, Τουρκία, Τσεχική Δημοκρατία, Φινλανδία.

[409] Μυλώση, Μ. (2015). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία, σελ. 301.

Η διασυνοριακή ροή των προσωπικών δεδομένων αντιμετωπίζεται στο άρθρο 14 του 3ου κεφαλαίου της Σύστασης R (99) 5. Πιο συγκεκριμένα, το κεφάλαιο 3, το οποίο προβλέπει κανόνες που αφορούν τους παρόχους υπηρεσιών του Διαδικτύου, αναφέρει στο άρθρο 14 τα προαπαιτούμενα βήματα πριν τη διαβίβαση των προσωπικών δεδομένων σε μία τρίτη χώρα. Εν πρώτοις, τονίζεται η ανάγκη παροχής συμβουλής (πχ από την αρμόδια αρχή) πριν τη διασυνοριακή διαβίβαση, ώστε να διαπιστωθεί αν η διαβίβαση είναι επιτρεπτή. Επιπλέον, η Σύσταση R (99) 5 επιλέγει να εστιάσει στο εργαλείο της διασυνοριακής διαβίβασης μέσω του οποίου ο εισαγωγέας των δεδομένων παρέχει διασφαλίσεις για την προστασία τους [410].

Αναμφισβήτητα, το πλαίσιο της Σύστασης R (99) 5 για τις διασυνοριακές ροές των δεδομένων κινείται σε γενικές ρυθμίσεις και προβαίνει σε γενικές προτάσεις με στόχο να δοθεί έμφαση στα καίρια σημεία της.

6.6 Το πλαίσιο της Οικονομικής Συνεργασίας Ασίας-Ειρηνικού (APEC) για την ιδιωτικότητα και το σύστημα διασυνοριακών κανόνων για την ιδιωτικότητα (CBPR)

Η Οικονομική Συνεργασία Ασίας-Ειρηνικού (Asia-Pacific Economic Cooperation, APEC) είναι ένα περιφερειακό οικονομικό φόρουμ που ιδρύθηκε το 1989 με στόχο τη βέλτιστη αξιοποίηση της αλληλεπίδρασης της περιοχής της Ασίας και του Ειρηνικού[411] και αποτελείται από 21 μέλη[412].

Το πλαίσιο της Οικονομικής Συνεργασίας Ασίας-Ειρηνικού για την ιδιωτικότητα αποτελείται από εννέα κατευθυντήριες γραμμές με σκοπό την υιοθέτησή τους από τις εθνικές νομοθεσίες. Το πλαίσιο αυτό για την προστασία των προσωπικών δεδομένων αναθεωρήθηκε το 2015. Στο πεδίο των διασυνοριακών ροών των δεδομένων, οι αρχές αυτές διαπνέονται κυρίως από την αρχή της λογοδοσίας[413], η οποία αποτελεί παράλληλα και υποχρέωση του

[410] Committee of Ministers of the Council of Europe. (1999). Σύσταση R (99) 5 on the protection of privacy on the Internet. Διαθέσιμο στο: https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

[411] Βλ. https://www.apec.org/about-us/about-apec

[412] Τα μέλη της APEC αποτελούνται από τα εξής κράτη: Αυστραλία, Μπρουνέι Νταρουμσαλάμ, Καναδάς, Ινδονησία, Ιαπωνία, Δημοκρατία της Κορέας, Μαλαισία, Νέα Ζηλανδία, Φιλιππίνες, Σιγκαπούρη, Ταϊλάνδη, ΗΠΑ, Κινεζική Ταϊπέι, Χονγκ Κονγκ, Λαϊκή Δημοκρατία της Κίνας, Μεξικό, Παπούα Νέα Γουινέα, Χιλή, Περού, Ρωσία, Βιετνάμ.

[413] APEC. (2019). Cross-Border Privacy Rules System Policies, Rules and Guidelines. Διαθέσιμο στο: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

υπεύθυνου της επεξεργασίας των δεδομένων. Ειδικότερα το άρθρο 26, το οποίο φέρει τον τίτλο «*IX. Λογοδοσία*» αναφέρει ότι: «*…Όταν πρόκειται να γίνει μεταφορά προσωπικών πληροφοριών σε άλλο πρόσωπο ή οργανισμό, εγχώρια ή διεθνώς, ο υπεύθυνος της επεξεργασίας των προσωπικών πληροφοριών πρέπει να λάβει τη συγκατάθεση του ατόμου ή να ασκήσει τη δέουσα επιμέλεια και να λάβει εύλογα μέτρα για να διασφαλίσει ότι ο αποδέκτης ή ο οργανισμός θα προστατεύει τις πληροφορίες με συνέπεια σύμφωνα με αυτές τις Αρχές».*

Το Σύστημα Διασυνοριακών Κανόνων Προστασίας Προσωπικών Δεδομένων (Cross-Border Privacy Rules, CBPR)[414] [415], το οποίο ισχύει από το 2011 και αναθεωρήθηκε το 2019, είναι ένα πλαίσιο το οποίο αναπτύχθηκε από την APEC μέσω της δημιουργίας συγκεκριμένων προτύπων. Θα πρέπει να σημειωθεί ότι το σύστημα CBPR, στο οποίο συμμετέχουν επί του παρόντος εννέα κράτη[416], δεν έχει δεσμευτικό χαρακτήρα. Εντούτοις, οι εταιρείες των κρατών μελών της APEC τα οποία ανήκουν στο CBPR, δύνανται να επιλέγουν τη δυνατότητα πιστοποίησης στο πλαίσιο του συστήματος[417]. Αναλυτικότερα, το σύστημα CBPR περιλαμβάνει την ανεξάρτητη πιστοποίηση του οργανισμού που επιδιώκει τη συμμετοχή του στο σύστημα CBPR από έναν υπεύθυνο λογοδοσίας[418]. Αναμφισβήτητα, οι αρχές της APEC για την ιδιωτικότητα υιοθετούν την προσέγγιση στις διασυνοριακές ροές υπό το πρίσμα του εκάστοτε οργανισμού, δίνοντας έμφαση στην υποχρέωση λογοδοσίας.

Το σύστημα CBPR κινείται γύρω από τους κεντρικούς άξονες που αφορούν τη διαδικασία συμμετοχής των χωρών της APEC στο σύστημα, τη διαδικασία αναγνώρισης των υπεύθυνων λογοδοσίας, τη διαδικασία πιστοποίησης του εκάστοτε οργανισμού, καθώς και τον ρόλο των αρχών προστασίας των

[414] APEC. (2019). Cross-Border Privacy Rules System Policies, Rules and Guidelines. Διαθέσιμο στο: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

[415] Βλ. http://cbprs.org/about-cbprs/

[416] Τα μέλη του CBPR αποτελούνται από τα εξής κράτη: ΗΠΑ, Μεξικό, Ιαπωνία, Καναδάς, Σιγκαπούρη, Δημοκρατία της Κορέας, Αυστραλία, Κινεζική Ταϊπέι, Φιλιππίνες.

[417] OECD. (2020). Mapping approaches to cross-border data flows. Report for the G20 Digital Economy Task Force. Διαθέσιμο στο: https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1620464835&id=id&accname=guest&checksum=BCE1CCC78F3747D1386E1D0446E3B8CC

[418] Sullivan, C. (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. *computer law & security review*, *35*(4), 380-397.

προσωπικών δεδομένων[419]. Οι διαδικασίες περιγράφονται αναλυτικά στα άρθρα 29-42 του κειμένου του CBPR.

Πιο συγκεκριμένα, οι οργανισμοί που επιδιώκουν τη συμμετοχή τους στο σύστημα CBPR θα πρέπει να εφαρμόζουν τις πολιτικές και τις διαδικασίες όπως περιγράφονται στο σύστημα. Οι εν λόγω πολιτικές και πρακτικές για την προστασία της ιδιωτικότητας υπόκεινται στην αξιολόγηση ενός αναγνωρισμένου από την APEC αντιπροσώπου λογοδοσίας. Εφόσον ένας οργανισμός έχει πιστοποιηθεί, οι πολιτικές και οι πρακτικές καθίστανται δεσμευτικές ως προς τον συμμετέχοντα. Παράλληλα, η εκάστοτε αρμόδια αρχή διασφαλίζει τη συμμόρφωση με τις απαιτήσεις του συστήματος[420].

Θα πρέπει να σημειωθεί ότι, επί της ουσίας, οι πρακτικές και οι πολιτικές προστασίας των προσωπικών δεδομένων καταγράφονται από τους ίδιους τους οργανισμούς. Τα στοιχεία τα οποία θα καθορίσουν την προστασία των διαβιβαζόμενων δεδομένων υπόκεινται στην αυτοαξιολόγηση των οργανισμών. Αυτή επιτυγχάνεται μέσω της συμπλήρωσης ενός ερωτηματολογίου με γνώμονα, όπως είναι φυσικό, το πλαίσιο της προστασίας των προσωπικών δεδομένων της APEC (APEC Privacy Framework 2015)[421].

Συμπερασματικά, το σύστημα CBPR αποτελεί ένα λεπτομερές και με έμφαση στην πρακτική εφαρμογή διασυνοριακό εργαλείο των προσωπικών δεδομένων. Τα χαρακτηριστικά αυτά εξασφαλίζονται μέσω των αναλυτικών αναφορών στις απαιτούμενες διαδικασίες και στα βήματα που θα πρέπει να ακολουθηθούν για τη λήψη της πιστοποίησης. Η προστασία των διαβιβαζόμενων προσωπικών δεδομένων εδράζεται κατά αυτόν τον τρόπο στην ad hoc αντιμετώπιση του κάθε οργανισμού. Σε αντιστοιχία με το πλαίσιο προστασίας των προσωπικών δεδομένων της APEC, το οποίο συμπληρώνει το σύστημα CBPR, κεντρικό άξονα αποτελεί η αρχή της λογοδοσίας.

[419] APEC. (2019). Cross-Border Privacy Rules System Policies, Rules and Guidelines. Διαθέσιμο στο: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

[420] APEC. (2019). Cross-Border Privacy Rules System Policies, Rules and Guidelines. Διαθέσιμο στο: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

[421] Βλ. APEC. (2019). Cross-Border Privacy Rules System Policies, Rules and Guidelines. Διαθέσιμο στο: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

6.7 Το ψήφισμα της Μαδρίτης σχετικά με τα διεθνή πρότυπα για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής

Το ψήφισμα της Μαδρίτης (The International Standards on Privacy and Data Protection, Madrid Resolution)[422] εγκρίθηκε στις 5 Νοεμβρίου 2009 στην ετήσια συνάντηση της Διεθνούς Διάσκεψης των Επιτρόπων για την Προστασία των Δεδομένων και της Ιδιωτικής Ζωής (International Conference of Data Protection and Privacy Commissioners, ICDPPC). Πιο συγκεκριμένα, η Διάσκεψη αυτή αποτελεί ένα παγκόσμιο φόρουμ εμπειρογνωμόνων στο πεδίο της προστασίας των προσωπικών δεδομένων καθώς και των αρχών προστασίας και ιδρυμάτων[423]. Τα πρότυπα υιοθετήθηκαν το 2009 υπό την προεδρία της ισπανικής αρχής για την προστασία των προσωπικών δεδομένων (Spanish Data Protection Agency)[424]. Επισημαίνεται ότι λόγω της συμμετοχής και των αρχών προστασίας των προσωπικών δεδομένων εκτός της ΕΕ[425], το εν λόγω εργαλείο στο παρόν πόνημα έχει συμπεριληφθεί στα διεθνή και όχι στα ευρωπαϊκά εργαλεία τα οποία διέπουν τις διασυνοριακές ροές δεδομένων.

Τα προτεινόμενα πρότυπα δεν έχουν δεσμευτικό χαρακτήρα και στοχεύουν στην υιοθέτηση ενός διεθνώς ενοποιημένου θεσμικού πλαισίου για την προστασία των προσωπικών δεδομένων. Ως εκ τούτου, συνιστούν μία αξιοσημείωτη διεθνή θεσμική ρύθμιση, η οποία αποσκοπεί στον συγκερασμό των εθνικών νομοθεσιών για την προστασία των προσωπικών δεδομένων[426].

Τα πρότυπα διακρίνονται σε θεματικά κεφάλαια, σχετικά με τα βασικά στοιχεία που διέπουν την προστασία των προσωπικών δεδομένων. Ως προς τη ρύθμιση των διασυνοριακών ροών, αυτά περιλαμβάνονται στο κεφάλαιο 15 των προτύπων. Ειδικότερα, στην παρ. 1 αποτυπώνεται το γενικό πλαίσιο των διασυνοριακών ροών των δεδομένων, οι οποίες μπορούν να διεξάγονται όταν το

---

[422] AEPD, PFPDT. (2009). International Standards on the Protection of Personal Data and Privacy, *Madrid Resolution*. In *International Conference of Data Protection and Privacy Commissioners,* Agencia Española de Protección de Datos (AEPD) and Préposé fédéral à la protection des données et à la transparence (PFPDT), Madrid. Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_en.pdf

[423] OECD/IDB (2016). Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit. Διαθέσιμο στο: http://dx.doi.org/10.1787/9789264251823-en

[424] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p. 58.

[425] Βλ. AEPD, PFPDT. (2009). International Standards on the Protection of Personal Data and Privacy, *Madrid Resolution*. In *International Conference of Data Protection and Privacy Commissioners,* Agencia Española de Protección de Datos (AEPD) and Préposé fédéral à la protection des données et à la transparence (PFPDT), Madrid. Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_en.pdf

[426] Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p. 58.

κράτος εισαγωγής των δεδομένων διαθέτει κατ' ελάχιστο το επίπεδο της προστασίας των δεδομένων που απορρέει από τα πρότυπα. Επιπρόσθετα, οι διαβιβάσεις καθίστανται εφικτές, σύμφωνα με τα πρότυπα, όταν υφίστανται κατάλληλες συμβατικές ρήτρες (παρ. 2), δεσμευτικοί εταιρικοί κανόνες (παρ. 2), το συμφέρον του υποκειμένου των δεδομένων στο πλαίσιο συμβατικής σχέσης, το ζωτικό συμφέρον του υποκειμένου των δεδομένων ή άλλου προσώπου, οι σημαντικοί λόγοι δημοσίου συμφέροντος (παρ. 3). Παράλληλα, τα πρότυπα εκχωρούν την εξουσία στις εθνικές νομοθεσίες να επιτρέπουν στις εθνικές αρχές τον καθορισμό της πραγματοποίησης ή όχι των διεθνών διαβιβάσεων που εμπίπτουν στη δικαιοδοσία τους (παρ. 4).

Αξίζει να σημειωθεί ότι από την ανάλυση των διασυνοριακών μηχανισμών του κεφαλαίου 15 των προτύπων, διαφαίνεται η σχέση τόσο με την τότε ισχύουσα Οδηγία 95/46/ΕΚ, όσο και με τον ισχύοντα GDPR. Ειδικότερα, οι μηχανισμοί των παρ. 2 και 3 του κεφαλαίου 15 είναι αντίστοιχες της Οδηγίας 95/46/ΕΚ[427]. Ωστόσο, θα πρέπει να σημειωθεί ότι από το κεφάλαιο 15 των προτύπων απουσιάζει ο διασυνοριακός μηχανισμός (παρέκκλιση) της ρητής συγκατάθεσης του υποκειμένου των δεδομένων, ο οποίος ενυπάρχει διαχρονικά στο ευρωπαϊκό πλαίσιο της προστασίας των προσωπικών δεδομένων.

6.8 Συμπληρωματικός νόμος για την προστασία των προσωπικών δεδομένων της Δυτικοαφρικανικής Οικονομικής και Νομισματικής Ένωσης (ECOWAS)

Η Οικονομική Κοινότητα των κρατών της Δυτικής Αφρικής (Economic Community of West African States, ECOWAS)[428] που δημιουργήθηκε στις 28 Μαΐου 1975 με τη Συνθήκη του Λάγος, με στόχο την οικονομική ολοκλήρωση, αποτελείται από δεκαπέντε χώρες[429] οι οποίες βρίσκονται στην περιοχή της Δυτικής Αφρικής[430]. Το πρώτο κράτος-μέλος της ECOWAS, το οποίο υιοθέτησε εθνικό νόμο για την προστασία των προσωπικών δεδομένων, ήταν το Πράσινο Ακρωτήρι το 2001 με το νόμο No133/V/2001, ο οποίος περιείχε και τη

[427] Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p. 58.

[428] Βλ. https://www.ecowas.int/about-ecowas/basic-information/

[429] Τα μέλη της ECOWAS αποτελούνται από τα εξής κράτη: Μπενίν, Μπουρκίνα Φάσο, Πράσινο Ακρωτήριο, Γκάμπια, Γκάνα, Γουινέα, Γουινέα-Μπισσάου, Ακτή Ελεφαντοστού, Λιβερία, Μάλι, Νίγηρας, Νιγηρία, Σενεγάλη, Σιέρα Λεόνε, Τόγκο.

[430] Βλ. https://www.ecowas.int/member-states/

θεσμοθέτηση του πλαισίου των διασυνοριακών ροών των προσωπικών δεδομένων[431].

Ως απόρροια της αναθεώρησης της συνθήκης της ECOWAS, το 2008 αναδείχθηκε το ζήτημα της υιοθέτησης νόμων για την προστασία των προσωπικών δεδομένων[432]. Ο συμπληρωματικός νόμος για την προστασία των προσωπικών δεδομένων[433], που εγκρίθηκε από τα κράτη μέλη της ECOWAS το 2010, αφενός θεσπίζει το περιεχόμενο του εθνικού νόμου το οποίο πρέπει να υιοθετήσουν τα μέλη και αφετέρου υποδεικνύει την απαίτηση θέσπισης μιας εθνικής αρχής προστασίας των προσωπικών δεδομένων[434].

Πρόκειται για μία νομικά δεσμευτική περιφερειακή αλλά και διεθνή θεσμική ρύθμιση, αποτελώντας τη μοναδική ρύθμιση στην περιοχή της Αφρικής με αυτά τα χαρακτηριστικά[435]. Η διασυνοριακή ροή των προσωπικών δεδομένων αντιμετωπίζεται από τις παραγράφους 1 και 2 του άρθρου 36 του νόμου. Αναλυτικότερα, η παρ. 1 αναφέρει ότι: «*Ο υπεύθυνος επεξεργασίας των δεδομένων μεταφέρει προσωπικά δεδομένα σε μη μέλος της ECOWAS μόνο όταν η χώρα αυτή παρέχει επαρκές επίπεδο προστασίας για την ιδιωτικότητα, τις ελευθερίες και τα θεμελιώδη δικαιώματα των ατόμων σε σχέση με την επεξεργασία ή την πιθανή επεξεργασία των δεδομένων».*

Αρχικά, θα πρέπει να σημειωθεί ότι καθίσταται σαφής η ανάγκη διασυνοριακής συνεργασίας και αμοιβαιότητας μεταξύ των χωρών που απαρτίζουν την ECOWAS. Στην παράγραφο 1, τίθεται η διάκριση των μελών και μη μελών της κοινότητας σε σχέση με τις διασυνοριακές ροές δεδομένων με μία διατύπωση η οποία τονίζει την κατά παρέκκλιση διαβίβαση των προσωπικών δεδομένων. Πιο συγκεκριμένα, θα μπορούσε να υποστηριχθεί ότι η απαίτηση για επάρκεια του επιπέδου προστασίας των δεδομένων της τρίτης χώρας παραπέμπει στην προσέγγιση των νομοθεσιών αυτών που θεσπίζουν το ζήτημα των διασυνοριακών ροών των προσωπικών δεδομένων βάσει της τοποθεσίας.

---

[431] Orji, U. J. (2017). Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act. *International Data Privacy Law*, *7*(3), 179-189.

[432] Greenleaf, G., & Georges, M. (2014). African regional privacy instruments: Their effects on harmonization.

[433] Βλ. ECOWAS. (2010). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, adopted at the 37th session of the Authority of ECOWAS Heads of State and Government, (Abuja, 16 February 2010).

[434] Greenleaf, G., & Georges, M. (2014). African regional privacy instruments: Their effects on harmonization.

[435] Greenleaf, G., & Georges, M. (2014). African regional privacy instruments: Their effects on harmonization.

Επιπρόσθετα, ενώ είναι σαφές ότι η θέσπιση αλλά και οι διατάξεις του συμπληρωματικού νόμου στοχεύουν στην εναρμόνιση των νόμων των κρατών-μελών, οι διατάξεις της διασυνοριακής διαβίβασης ενθαρρύνουν ιδιαίτερα τη διασυνοριακή συνεργασία εντός της ECOWAS[436].

Παράλληλα, η παρ. 2 του άρθρου 36 εισάγει την απαίτηση της ενημέρωσης της αρχής προστασίας των προσωπικών δεδομένων πριν από τη διασυνοριακή εξαγωγή δεδομένων σε τρίτη χώρα εκτός της ECOWAS. Η διάταξη αυτή αφενός ενισχύει έμπρακτα την αρχή της λογοδοσίας του υπεύθυνου της επεξεργασίας και αφετέρου ενδυναμώνει τις εξουσίες των αρχών προστασίας των δεδομένων μέσω της προληπτικής προσέγγισης των κινδύνων.

6.9 Οι κανόνες της Κοινότητας για την Ανάπτυξη της Μεσημβρινής Αφρικής (HIPSSA)

Η Κοινότητα για την Ανάπτυξη της Μεσημβρινής Αφρικής (Southern African Development Community, SADC) ιδρύθηκε το 1980, αποτελώντας έναν διακυβερνητικό οργανισμό με 16 μέλη[437] που στοχεύει στην προώθηση της βιώσιμης και ισότιμης κοινωνικοοικονομικής ανάπτυξης[438].

Οι κανόνες της Κοινότητας για την Ανάπτυξη της Μεσημβρινής Αφρικής (SADC Model Law on Data Protection)[439] του 2013 αναπτύχτηκαν στο πλαίσιο του προγράμματος HIPSSA (Support to the Harmonisation of ICT Policies in Sub-Sahara Africa)[440], το οποίο χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union, ITU).

Η διασυνοριακή ροή των προσωπικών δεδομένων αντιμετωπίζεται στους κανόνες της Κοινότητας για την Ανάπτυξη της Μεσημβρινής Αφρικής στα άρθρα 43-45. Συλλήβδην, ο πρότυπος νόμος της SADC διακρίνει σε δύο περιπτώσεις τη

---

[436] Orji, U. J. (2017). Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act. *International Data Privacy Law*, *7*(3), 179-189.

[437] Τα μέλη της SADC αποτελούνται από τα εξής κράτη: Ανγκόλα, Μποτσουάνα, Ένωση των Κομορών, Λαϊκή Δημοκρατία του Κονγκό, Εσουατίνι, Λεσότο, Μαδαγασκάρη, Μαλάουι, Μαυρίκιος, Μοζαμβίκη, Ναμίμπια, Σεϋχέλλες, Νότια Αφρική, Τανζανία, Ζάμπια, Ζιμπάμπουε.

[438] Βλ. https://www.sadc.int/about-sadc/overview/sadc-facts-figures/

[439] HIPSSA–Data Protection: SADC Model Law. (2013). Διαθέσιμο στο: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[440] Βλ. http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

ρύθμιση των διασυνοριακών ροών των προσωπικών δεδομένων. Αναλυτικότερα, το άρθρο 43 ρυθμίζει το πλαίσιο των διασυνοριακών ροών των δεδομένων μεταξύ των κρατών μελών της SADC τα οποία όμως έχουν μεταφέρει τους εν λόγω κανόνες στην εθνική νομοθεσία. Τα άρθρα 44 και 45 καταγράφουν το πλαίσιο των διασυνοριακών ροών από ένα κράτος μέλος της SADC που έχει εφαρμόσει την εν λόγω νομοθεσία σε κράτος που δεν αποτελεί μέλος της SADC ή σε κράτος μέλος της SADC που δεν έχει μεταφέρει στο εθνικό δίκαιο τους εν λόγω κανόνες[441]. Καθίσταται προφανής, από τη διατύπωση των κανόνων, η προσπάθεια ενθάρρυνσης των μελών της SADC να θεσπίσουν εθνικούς νόμους σε αντιστοιχία με τους κανόνες του πρότυπου νόμου. Σε διαφορετική περίπτωση, στον τομέα των διεθνών διαβιβάσεων θα αντιμετωπίζονται ομοίως με τα κράτη που δεν ανήκουν στην Κοινότητα (τρίτα κράτη).

Κατά την πρώτη περίπτωση, γενικά οι διασυνοριακές ροές των δεδομένων δύνανται να πραγματοποιούνται με την επιφύλαξη των διατάξεων που αναφέρονται στο άρθρο 43. Κατά τη δεύτερη περίπτωση, η διαβίβαση των δεδομένων πραγματοποιείται μόνο εάν εξασφαλίζεται επαρκές επίπεδο προστασίας από τη χώρα εισαγωγής και όταν η μεταφορά διενεργείται μόνο εντός του ορίου της αρμοδιότητας του υπεύθυνου της επεξεργασίας (άρθρο 44). Το άρθρο 45 περιγράφει την αντιμετώπιση των διασυνοριακών ροών των δεδομένων όταν δεν υφίσταται επαρκές επίπεδο προστασίας των δεδομένων στη χώρα εισαγωγής. Ειδικότερα, η παρ. 1 του άρθρου 45 απαριθμεί έξι μηχανισμούς/περιπτώσεις στις οποίες μπορεί να εδράζεται η διεθνής διαβίβαση.

Οι παρεκκλίσεις αυτές περιλαμβάνουν: «τη σαφή συγκατάθεση του υποκειμένου των δεδομένων, την περίπτωση κατά την οποία η διαβίβαση είναι απαραίτητη κατά το προσυμβατικό στάδιο ή κατά την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας, την περίπτωση κατά την οποία η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υπεύθυνου επεξεργασίας και τρίτου μέρους προς το συμφέρον του υποκειμένου των δεδομένων, την ύπαρξη λόγων δημοσίου συμφέροντος ή τη σύσταση, άσκηση ή υπεράσπιση νομικών αξιώσεων, την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων, τη μεταφορά των δεδομένων στο πλαίσιο της λειτουργίας ενός μητρώου, σύμφωνα με τους κείμενους νόμους και κανονισμούς».

Στην παρ. 2 του άρθρου 45 καταγράφεται το εργαλείο των κατάλληλων εγγυήσεων από τον υπεύθυνο της επεξεργασίας των διαβιβαζόμενων δεδομένων.

[441] Makulilo, A. B. (Ed.). (2016). *African data privacy laws* (Vol. 33). Cham: Springer.

Ειδικότερα, γίνεται ενδεικτική αναφορά στον διασυνοριακό μηχανισμό των κατάλληλων συμβατικών ρητρών.

Κατά συνέπεια, θα μπορούσε να υποστηριχθεί ότι οι κανόνες της Κοινότητας για την Ανάπτυξη της Μεσημβρινής Αφρικής εμφανίζουν αντιστοιχία με την ευρωπαϊκή νομοθεσία στο πεδίο των διασυνοριακών ροών των δεδομένων, ιδίως λόγω της διατύπωσης των έξι παρεκκλίσεων και των κατάλληλων εγγυήσεων όταν δεν υφίσταται η περίπτωση της επάρκειας της τρίτης χώρας.

6.10 Οι Αρχές προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων του Οργανισμού Αμερικανικών Κρατών (OAS)

Ο Οργανισμός Αμερικανικών Κρατών (Organization of American States, OAS) υφίσταται από το 1948 με την υπογραφή στη Μπογκοτά του Χάρτη του OAS από 21 κράτη (εν συνεχεία προσχώρησαν ακόμη 14 μέλη[442]). Το 2015 η Διαμερικανική Νομική Επιτροπή (Inter-American Juridical Committee, IAJC) του OAS ενέκρινε την έκθεση[443] που αφορά την προστασία των προσωπικών δεδομένων με στόχο να διαδραματίσει τον ρόλο των πρότυπων κανόνων για τα εθνικά δίκαια των χωρών του OAS[444].

Μεταξύ των δώδεκα αρχών του OAS για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, η ενδέκατη αρχή αναφέρεται στη διασυνοριακή ροή των δεδομένων και φέρει τον τίτλο: «*Διασυνοριακή ροή των δεδομένων και λογοδοσία*». Κεντρική απαίτηση της ενδέκατης αρχής αποτελεί η θέσπιση εργαλείων από τα κράτη μέλη και η συνεργασία τους στο πεδίο της λογοδοσίας του υπεύθυνου της επεξεργασίας, ο οποίος δρα σε περισσότερες δικαιοδοσίες. Παράλληλα, στις αρχές αναγνωρίζονται τρία βασικά ζητήματα στο πεδίο των διασυνοριακών ροών των δεδομένων. Ειδικότερα, το πρώτο αφορά στη διαφοροποίηση των εθνικών νομοθεσιών των κρατών, το δεύτερο στο δικαίωμα διακρατικής πρόσβασης στα προσωπικά δεδομένα και το τρίτο στο γεγονός πως η

[442]Τα κράτη τα οποία έχουν επικυρώσει τον χάρτη της OAS είναι τα εξής: Αργεντινή, Βολιβία, Βραζιλία, Χιλή, Κολομβία, Κόστα Ρίκα, Κούβα, Δομινικανή Δημοκρατία, Ισημερινός, Ελ Σαλβαδόρ, Γουατεμάλα, Αϊτή, Ονδούρα, Μεξικό, Νικαράγουα, Παναμάς, Παραγουάη, Περού, Ηνωμένες Πολιτείες Αμερικής, Ουρουγουάη, Βενεζουέλα, Μπαρμπάντος, Τρινιντάντ και Τομπάγκο, Τζαμάικα, Γρενάδα, Σουρινάμ, Δομινίκα, Αγία Λουκία, Αντίγκουα και Μπαρμπούντα, Άγιος Βικέντιος και Γρεναδίνες, Μπαχάμες, Άγιος Χριστόφορος και Νέβις, Καναδάς, Μπελίζ, Γουιάνα.

[443]OAS. (2015). Protection of Personal Data. Διαθέσιμο στο: http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf

[444]Βλ. https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-119/15

επεξεργασία των προσωπικών δεδομένων συμβάλλει στην ανάπτυξη και στην καινοτομία[445].

Επί του πρακτέου, οι αρχές επιτρέπουν εν γένει τις διεθνείς διαβιβάσεις δεδομένων μεταξύ των νομοθεσιών που περιλαμβάνουν τις αρχές προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων του OAS, ή αντίστοιχο επίπεδο προστασίας, και στην περίπτωση που οι υπεύθυνοι της επεξεργασίας υιοθετούν μέτρα για τη διαβίβαση σύμφωνα με αυτές τις αρχές. Η ενδέκατη αρχή διαπνέεται από την αποφυγή της εξωεδαφικής εφαρμογής του εθνικού δικαίου. Ειδικότερα, αναφέρεται ότι θα πρέπει να παραλείπεται η επιβολή ενός περιορισμού «αδικαιολόγητα αυστηρού» ο οποίος επιτάσσει εξωεδαφική εφαρμογή του δικαίου μίας χώρας.

Παράλληλα, αναδεικνύεται, μέσω ολόκληρου του κειμένου των αρχών, η απαίτηση της συνεργασίας των μελών στον τομέα της θέσπισης αμοιβαίων κανόνων λογοδοσίας για την εξάλειψη των περιορισμών στη διασυνοριακή ροή των δεδομένων, με μία ανάλυση του ρόλου των διασυνοριακών ροών στη σύγχρονη τεχνολογία και οικονομία.

Συμπερασματικά, θα πρέπει να σημειωθεί ότι οι αρχές του OAS προωθούν την αρχή της λογοδοσίας στο πεδίο των διασυνοριακών ροών, την αποφυγή των υπέρμετρων περιορισμών στη διασυνοριακή ροή και την αποτροπή της εξωεδαφικής εφαρμογής των νομοθεσιών για την προστασία των προσωπικών δεδομένων. Καθίσταται, λοιπόν, σαφής η υιοθέτηση από τη Διαμερικανική Νομική Επιτροπή του OAS της προσέγγισης της διασυνοριακής ροής δεδομένων με κριτήριο τους οργανισμούς και ως εκ τούτου την υποχρέωση λογοδοσίας, η οποία διαφέρει από την ευρωπαϊκή προσέγγιση, που υιοθετεί το κριτήριο της τοποθεσίας και της εξωεδαφικής εμβέλειας, όπου απαιτείται.

6.11 Συνολική και Προοδευτική Συμφωνία για την Εταιρική Σχέση των Χωρών του Ειρηνικού

Η Συνολική και Προοδευτική Συμφωνία για την Εταιρική Σχέση των Χωρών του Ειρηνικού (Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP)[446] αποτελεί μια συμφωνία για την ελεύθερη διεξαγωγή του εμπορίου μεταξύ: Αυστραλίας, Μπρουνέι Νταρουσαλάμ, Καναδά, Χιλής,

[445]Βλ. OAS. (2015). Protection of Personal Data. Διαθέσιμο στο: http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf

[446]Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). (2018). Διαθέσιμο στο: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents.

Ιαπωνίας, Μαλαισίας, Μεξικού, Περού, Νέας Ζηλανδίας, Σιγκαπούρης και Βιετνάμ. Η συμφωνία υπεγράφη στις 8 Μαρτίου 2018 στο Σαντιάγο της Χιλής[447] και στο άρθρο 1 ενσωματώνει το μεγαλύτερο μέρος της Συμφωνίας για την Εταιρική Σχέση των Χωρών του Ειρηνικού (Trans-Pacific Partnership Agreement, TPP)[448], στο κείμενο της οποίας περιλαμβάνονται οι διατάξεις που αφορούν τη διασυνοριακή ροή των δεδομένων.

Αναλυτικότερα, το άρθρο 14.11, το οποίο φέρει τον τίτλο: *«Διασυνοριακή ροή πληροφοριών με ηλεκτρονικά μέσα»,* αναφέρεται στην εθνική νομοθεσία των κρατών για τη διασυνοριακή ροή των προσωπικών δεδομένων. Εν πρώτοις, στην παρ. 1 του άρθρο 14.11 της Συμφωνίας γίνεται αναφορά στην ύπαρξη των διαφορετικών νομοθεσιών που διέπουν τη διαβίβαση δεδομένων και της αποδοχής της διαφοροποίησης αυτής. Ωστόσο, η παρ. 2 θέτει μία γενική ρύθμιση των διασυνοριακών ροών μεταξύ των μερών της συμφωνίας, επιτρέποντας τες στο πλαίσιο των επιχειρηματικών δραστηριοτήτων των υποκειμένων των δεδομένων. Περιορισμός στη γενική αυτή ρύθμιση τίθεται από τις περ. α και β της παρ. 3. Πιο συγκεκριμένα, επιτρέπει τον περιορισμό των διασυνοριακών ροών όταν αφενός δεν αποτελεί «αυθαίρετη ή αδικαιολόγητη διάκριση ή συγκαλυμμένο περιορισμό στο εμπόριο» και αφετέρου «δεν επιβάλλει μεγαλύτερους περιορισμούς στη διαβίβαση πληροφοριών από αυτούς που απαιτούνται για την επίτευξη του στόχου».

Η υιοθέτηση της προσέγγισης της αποφυγής των περιορισμών στη διασυνοριακή ροή των δεδομένων, και ιδιαίτερα με την αρωγή της αρχής της αναλογικότητας ως προς τον επιδιωκόμενο σκοπό, έρχεται σε αντιστοιχία με την εμπορική συμφωνία GATS. Παράλληλα, θα πρέπει να αναφερθεί ότι άμεση σχέση με το πεδίο των διασυνοριακών ροών φέρει η εδαφική εμβέλεια μίας νομοθεσίας. Ως εκ τούτου, είναι απαραίτητο να σημειωθεί ότι στο άρθρο 14.13 παρ. 2 τονίζεται η αποφυγή της απαίτησης εγκατάστασης υπολογιστικών συστημάτων διαχείρισης των δεδομένων σε ένα κράτος ως προϋπόθεση της διεξαγωγής επιχειρηματικών δραστηριοτήτων σε αυτή τη χώρα[449]. Από την εν λόγω διάταξη γίνεται εμφανής η προσέγγιση που υιοθετεί η συμφωνία, ως προς τη διασυνοριακή ροή των δεδομένων, η οποία έρχεται σε αντίθεση με το σχήμα της προστασίας βάσει της τοποθεσίας. Αναλυτικότερα, μία νομοθεσία που

[447]Βλ.https://www.abf.gov.au/importing-exporting-and-manufacturing/free-trade-agreements/comprehensive-and-progressive-agreement-for-trans-pacific-partnership

[448]Trans-Pacific Partnership Agreement (TPP). (2016). Διαθέσιμο στο: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents

[449] Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

βασίζεται στο κριτήριο της τοποθεσίας των δεδομένων επιδιώκει την παραμονή των δεδομένων εντός των συνόρων δικαιοδοσίας της, γεγονός το οποίο δύναται να συντελέσει στην υποχρέωση τοπικής επεξεργασίας των δεδομένων και ως εκ τούτου να αντιβαίνει στην παρ. 2 του άρθρου 14.13.

Πίνακας 3. Οι διατάξεις για τη διασυνοριακή ροη δεδομένων στις διεθνείς ρυθμίσεις

ΤΙΤΛΟΣ ΘΕΣΜΙΚΗΣ ΡΥΘΜΙΣΗΣ	ΔΙΑΤΑΞΕΙΣ ΓΑ ΤΗ ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ ΔΕΔΟΜΕΝΩΝ
Κατευθυντήριες γραμμές του ΟΟΣΑ από το 1980 (καταργήθηκε)	Παράγραφοι 15 έως 18
Αναθεωρημένες Κατευθυντήριες γραμμές του ΟΟΣΑ το 2013	Παράγραφοι 16 έως 18 και παράγραφος 6
Η σύμβαση 108/1981 του Συμβουλίου της Ευρώπης **Πρόσθετο πρωτόκολλο 181/2001 (καταργήθηκαν)**	Άρθρο 12 Άρθρο 2
Εκσυγχρονισμένη Σύμβαση 108 το 2018	Άρθρο 14
Οι κατευθυντήριες γραμμές προστασίας προσωπικών δεδομένων σε αυτοματοποιημένα αρχεία της Γενικής Συνέλευσης των Ηνωμένων Εθνών του 1990	Άρθρο 9
Η Σύσταση R (99) 5 της Επιτροπής Υπουργών του Συμβουλίου της Ευρώπης του 1999	Άρθρο 14 του 3ου κεφαλαίου
Το πλαίσιο της Οικονομικής Συνεργασίας Ασίας-Ειρηνικού (APEC) για την ιδιωτικότητα το 2005 (αναθεωρήθηκε το 2015) **Σύστημα διασυνοριακών κανόνων για την ιδιωτικότητα (CBPR) το 2011 (αναθεωρήθηκε το 2019)**	Άρθρο 26

Το ψήφισμα της Μαδρίτης σχετικά με τα διεθνή πρότυπα για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής (Madrid Resolution) το 2009	Κεφάλαιο 15
Συμπληρωματικός νόμος για την προστασία των προσωπικών δεδομένων της Δυτικοαφρικανικής Οικονομικής και Νομισματικής Ένωσης (ECOWAS) το 2010	Άρθρο 36
Οι κανόνες της Κοινότητας για την Ανάπτυξη της Μεσημβρινής Αφρικής (HIPSSA) το 2013	Άρθρα 43-45
Οι Αρχές προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων του Οργανισμού Αμερικανικών Κρατών (OAS) το 2015	Ενδέκατη αρχή
Η Συνολική και Προοδευτική Συμφωνία για την Εταιρική Σχέση των Χωρών του Ειρηνικού το 2018	Άρθρο 14.11

ΚΕΦΑΛΑΙΟ 7. ΕΘΝΙΚΕΣ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΔΙΑΣΥΝΟΡΙΑΚΗΣ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΠΑΓΚΟΣΜΙΟ ΕΠΙΠΕΔΟ

7.1 Εισαγωγή

Σύμφωνα με τα στοιχεία[450] της Διάσκεψης των Ηνωμένων Εθνών για το Εμπόριο και την Ανάπτυξη (United Nations Conference on Trade and Development, UNCTAD), το ποσοστό των κρατών παγκοσμίως που διαθέτουν νομοθεσία για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας κυμαίνεται στο 66 %. Παράλληλα, σύμφωνα με τα ίδια στοιχεία, 10 % των κρατών διαθέτει στον τομέα αυτό σχέδια/προτάσεις νομοθετικών ρυθμίσεων. Επομένως, υπό το πρίσμα των διεθνών νόμων για την προστασία των προσωπικών δεδομένων, καθίσταται ιδιαίτερα σημαντική τόσο η εξακρίβωση των εθνικών νόμων των χωρών όσο και η ανάλυση του περιεχομένου τους.

Η διασυνοριακή ροή των δεδομένων, και ειδικότερα των οικονομικών, αποτελεί ένα ζήτημα με διακρατική εμβέλεια, επιτάσσοντας πολλές φορές την εξακρίβωση του επιπέδου προστασίας των δεδομένων τρίτων κρατών. Ως εκ τούτου, στο παρόν κεφάλαιο θα παρουσιαστεί η ρύθμιση της διασυνοριακής ροής των προσωπικών δεδομένων σε επιλεγμένα κράτη, στοχεύοντας στην κάλυψη ενός ευρέος γεωγραφικού φάσματος. Παράλληλα, θα πρέπει στο σημείο αυτό να διευκρινιστεί ότι, λόγω της αμφίδρομης διάστασης των διασυνοριακών ροών των προσωπικών δεδομένων, οι νομοθετικές ρυθμίσεις των κρατών του παρόντος κεφαλαίου αφορούν τη θέση τους ως εξαγωγείς των προσωπικών δεδομένων.

7.2 Ρυθμίσεις σε επιλεγμένες χώρες της Ασίας

7.2.1 Ηνωμένα Αραβικά Εμιράτα

Σε γενικές γραμμές, σύμφωνα με το άρθρο 379 του Ποινικού Κώδικα (Federal Law No. 3) ο οποίος ισχύει στα Ηνωμένα Αραβικά Εμιράτα, τα προσωπικά δεδομένα μπορούν να αποκαλυφθούν αποκλειστικά κατόπιν συναίνεσης του υποκειμένου των δεδομένων ή σχετικής νομοθετικής πρόβλεψης. Ειδικότερα, τα δεδομένα των καταναλωτών, σύμφωνα με τον Κανονισμό εγκαταστάσεων αποθηκευμένης αξίας (Stored Value Facilities Regulation), θα πρέπει να διατηρούνται εντός της επικράτειας και να διατίθενται μόνο σε συγκεκριμένους πελάτες, στην Κεντρική Τράπεζα, σε άλλες ρυθμιστικές αρχές μετά από

[450] Βλ. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

προηγούμενη έγκριση της Κεντρικής Τράπεζας ή με δικαστική απόφαση (Άρθρο 10 παρ. 6)[451].

7.2.2 Ιαπωνία

Στην Ιαπωνία από το 2017 ισχύει ο νόμος για την προστασία των προσωπικών πληροφοριών (Act on the Protection of Personal Information)[452]. Η τροποποίηση του 2020, η οποία ενισχύει το ζήτημα της προστασίας των διασυνοριακών ροών με την προσθήκη των παρ. 2 και 3 στο άρθρο 24 του νόμου για την προστασία των προσωπικών πληροφοριών του 2016, προβλέπει στο άρθρο 24 τις διασυνοριακές ροές των δεδομένων και θα τεθεί σε ισχύ τον Απρίλιο του 2022.

Καταρχάς, η προστασία των διαβιβαζόμενων προσωπικών δεδομένων διασφαλίζεται με την απαίτηση της παροχής ισοδύναμου συστήματος προστασίας των προσωπικών δεδομένων, στη χώρα εισαγωγής των δεδομένων, με αυτό της Ιαπωνίας[453]. Στην περίπτωση της διασυνοριακής μεταφοράς των δεδομένων που βασίζεται στη συγκατάθεση των υποκειμένων των δεδομένων, θα πρέπει τα υποκείμενα των δεδομένων να λαμβάνουν σχετικές πληροφορίες με τη διαβίβαση, όπως ορίζεται στην παράγραφο 2 του άρθρου 24. Παράλληλα, στην περίπτωση της διασυνοριακής διαβίβασης που βασίζεται στο πλαίσιο ενός συστήματος προστασίας των προσωπικών δεδομένων (π.χ. εκτέλεση σύμβασης), η παρ. 3 του άρθρου 24 θέτει την απαίτηση διασφάλισης της συνέχισης της προστασίας των προσωπικών δεδομένων[454].

7.2.3 Ινδία

Η προστασία των προσωπικών δεδομένων στο πλαίσιο των διασυνοριακών ροών των δεδομένων στην Ινδία προβλέπεται στο άρθρο 7 (Μεταφορά των πληροφοριών) των Κανόνων για την Τεχνολογία των Πληροφοριών 2011 (The Information Technology Rules 2011)[455].

---

[451] Βλ. Piper, D. L. A. (2021). *Data protection laws of the world: full handbook*. DLA Piper.

[452] Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature, p 239.

[453] Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature, p 251.

[454] Hiroyuki Tanaka. (2021). Japan updates enforcement rules for amended APPI. Διαθέσιμο στο: https://iapp.org/news/a/japan-updates-enforcement-rules-for-amended-appi/

[455] Βλ. Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature, p 158.

Πιο συγκεκριμένα, το άρθρο 7 επιτρέπει εν πρώτοις τη μεταφορά των προσωπικών δεδομένων, ευαίσθητων και μη, σε δύο περιπτώσεις. Η πρώτη περίπτωση αφορά τους εισαγωγείς των προσωπικών δεδομένων που βρίσκονται εντός της Ινδίας, ενώ η δεύτερη περίπτωση περιλαμβάνει τους εισαγωγείς των δεδομένων που βρίσκονται σε χώρες με αντίστοιχο επίπεδο προστασίας των προσωπικών δεδομένων με αυτό που θέτουν οι Κανόνες της Ινδίας. Επιπρόσθετα, η διασυνοριακή μεταφορά των προσωπικών δεδομένων επιτρέπεται όταν είναι απαραίτητη για την εκτέλεση έγκυρης σύμβασης και όταν το υποκείμενο των δεδομένων έχει παράσχει τη συγκατάθεσή του για τη μεταφορά των δεδομένων.

7.2.4 Ισραήλ

Η διασυνοριακή μεταφορά των προσωπικών δεδομένων στο Ισραήλ διέπεται από τους Κανονισμούς προστασίας προσωπικών δεδομένων «Μεταφορά δεδομένων σε βάσεις δεδομένων στο εξωτερικό», 5761-2001 (Privacy Protection Regulations «Transfer of Data to Databases Abroad», 5761-2001)[456]. Ειδικότερα, το κεφάλαιο 2 του νόμου 5761-2001 περιλαμβάνει αναλυτικά τις οκτώ περιπτώσεις σύμφωνα με τις οποίες δύναται να πραγματοποιηθεί μία διασυνοριακή διαβίβαση προσωπικών δεδομένων εκτός του Ισραήλ.

Αναλυτικότερα, το κεφάλαιο 2 εκκινεί από την περίπτωση της συγκατάθεσης του υποκειμένου των δεδομένων ως πρώτη περίπτωση και προχωρά στη δεύτερη περίπτωση, στην οποία δεν δύναται να δοθεί η εν λόγω συγκατάθεση και η μεταφορά είναι «ζωτικής σημασίας για την προστασία της υγείας και της φυσικής ευεξίας του ατόμου». Επιπρόσθετα, κατά την τρίτη περίπτωση, τα δεδομένα μπορούν να διαβιβάζονται σε «εταιρεία υπό τον έλεγχο του κατόχου της βάσης δεδομένων από την οποία προέρχονται τα δεδομένα και έχει εγγυηθεί την προστασία τους μετά τη μεταφορά». Ακόμη, η περίπτωση 4 αναφέρεται στη μεταφορά η οποία βασίζεται στη «δέσμευση του εισαγωγέα των δεδομένων ως απόρροια της συμφωνίας με τον κάτοχο της βάσης δεδομένων από την οποία τα δεδομένα μεταφέρονται, να συμμορφώνεται με τους όρους ιδιοκτησίας και χρήσης των δεδομένων που ισχύουν για μια βάση δεδομένων στο Ισραήλ»[457]. Παράλληλα, η πέμπτη προϋπόθεση της μεταφοράς αναφέρεται στην περίπτωση της «δημοσιοποίησης ή του δημοσίου ελέγχου από νομική αρχή των δεδομένων». Επιπλέον, η έκτη περίπτωση περιλαμβάνει τη «ζωτικής σημασίας

[456] Βλ. Piper, D. L. A. (2021). *Data protection laws of the world: full handbook*. DLA Piper.

[457] Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001.

για τη δημόσια ασφάλεια» διαβίβαση, ενώ η έβδομη την υποχρεωτική διαβίβαση στο πλαίσιο του νόμου του Ισραήλ[458].

Η όγδοη και τελευταία περίπτωση της διασυνοριακής μεταφοράς των δεδομένων αναφέρεται στις περιπτώσεις τρίτων χωρών, στις οποίες επιτρέπεται η μεταφορά των δεδομένων. Οι δύο πρώτες περιπτώσεις αναφέρονται στα συμβαλλόμενα κράτη της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα και στα κράτη που μπορούν να λαμβάνουν προσωπικά δεδομένα από τα κράτη-μέλη της ΕΕ με τους ίδιους όρους. Θα πρέπει να σημειωθεί ότι οι εν λόγω διατάξεις σχετίζονται άμεσα με την απόφαση επάρκειας για το Ισραήλ, ως προς τις διεθνείς διαβιβάσεις, η οποία εξεδόθη από την Ευρωπαϊκή Επιτροπή[459]. Τέλος, διεθνείς διαβιβάσεις δεδομένων μπορούν να πραγματοποιούνται κατόπιν επίτευξης αμοιβαίας συμφωνίας για εφαρμογή των αρχών προστασίας των δεδομένων[460].

7.2.5 Κίνα

Η προστασία των προσωπικών δεδομένων στην Κίνα διέπεται από τον Νόμο για την Κυβερνοασφάλεια (Cybersecurity Law), που θεσπίστηκε στις 7 Νοεμβρίου 2016[461].

Το άρθρο 37 του Νόμου για την Κυβερνοασφάλεια προβλέπει την απαίτηση για τους «φορείς εκμετάλλευσης κρίσιμων πληροφοριών, οι οποίοι συλλέγουν ή παράγουν προσωπικές πληροφορίες ή σημαντικά δεδομένα κατά τη διάρκεια δραστηριοτήτων στην Κίνα, να τα αποθηκεύουν εντός της Κίνας». Παράλληλα, μπορούν να εξαχθούν δεδομένα εκτός της Κίνας όταν κρίνεται εκ των πραγμάτων απαραίτητο και αφού έχει αξιολογηθεί η ασφάλεια αυτής της διαβίβασης[462] [463].

---

[458] Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001.

[459] 2011/61/ΕΕ: Απόφαση της Επιτροπής, της 31ης Ιανουαρίου 2011, σχετικά με την επάρκεια, σύμφωνα με την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της προστασίας των δεδομένων προσωπικού χαρακτήρα από το Κράτος του Ισραήλ όσον αφορά την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32011D0061

[460] Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001.

[461] Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way Between the US and the EU?. *Penn St. JL & Int'l Aff.*, *8*, 49.

[462] Cybersecurity Law of the People’s Republic of China.

7.2.6 Τουρκία

Ο νόμος στην Τουρκία για την προστασία των προσωπικών δεδομένων No. 6698 (Law on the Protection of Personal Data No. 6698) δημοσιεύτηκε στις 7 Απριλίου 2016[464]. Οι διεθνείς μεταφορές των προσωπικών δεδομένων θεσπίζονται στο άρθρο 9 του νόμου.

Αναλυτικότερα, οι διεθνείς διαβιβάσεις προσωπικών δεδομένων μπορούν να λάβουν χώρα υπό το πλαίσιο τριών προϋποθέσεων που αναφέρονται στο νόμο. Η πρώτη περίπτωση περιλαμβάνει τη ρητή συγκατάθεση του υποκειμένου των δεδομένων (άρθρο 9 παρ. 1). Επιπλέον, η διαβίβαση επιτρέπεται και χωρίς τη ρητή συγκατάθεση του υποκειμένου των δεδομένων, όταν ισχύουν οι προϋποθέσεις των άρθρων 5 παρ. 2[465] και 6 παρ. 3[466] του νόμου, σε συνδυασμό με την αναγνώριση του αντίστοιχου επιπέδου προστασίας των δεδομένων στην τρίτη χώρα από το Συμβούλιο Προστασίας Προσωπικών Δεδομένων (άρθρο 9 παρ. 2 περ. α). Κατά την τρίτη περίπτωση, εάν η τρίτη χώρα δεν έχει εγκριθεί από το Συμβούλιο ως επαρκής, τότε δεσμεύονται οι υπεύθυνοι επεξεργασίας των δεδομένων στην Τουρκία και στο εξωτερικό, εγγράφως, για την παροχή επαρκούς επιπέδου προστασίας και το Συμβούλιο δύναται να εγκρίνει αυτήν τη διαβίβαση, ενώ ισχύουν παράλληλα και οι προϋποθέσεις των άρθρων 5 παρ. 2 και 6 παρ. 3 του νόμου (άρθρο 9 παρ. 2 περ. β)[467].

7.3 Ρυθμίσεις σε επιλεγμένες χώρες της Αφρικής

7.3.1 Νότια Αφρική

Η Νότια Αφρική θέσπισε τον νόμο για την Προστασία των Προσωπικών Πληροφοριών (Protection of Personal Information Act, POPI) το 2013[468]. Ο

---

[463] Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way Between the US and the EU?. *Penn St. JL & Int'l Aff., 8,* 49.

[464] Helvacioglu, A. D., & Stakheyeva, H. (2017). The tale of two data protection regimes: The analysis of the recent law reform in Turkey in the light of EU novelties. *Computer law & security review*, *33*(6), 811-824.

[465] Το άρθρο 5 παρ. 2 του Law on the Protection of Personal Data No. 6698 αναφέρεται στις περιπτώσεις νόμιμης επεξεργασίας χωρίς τη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

[466] Το άρθρο 6 παρ. 3 του Law on the Protection of Personal Data No. 6698 αναφέρεται στις περιπτώσεις νόμιμης επεξεργασίας ειδικών κατηγοριών προσωπικών δεδομένων χωρίς τη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

[467] Kişisel Verileri Koruma Kurumu, KVKK. (2019). Data Protection in Turkey. Διαθέσιμο στο: https://www.kvkk.gov.tr/Search?keyword=data%20protection%20in%20turkey&langText=en

[468] Makulilo, A. B. (Ed.). (2016). *African data privacy laws* (Vol. 33). Cham: Springer.

νόμος αυτός προβλέπει τις διασυνοριακές ροές των προσωπικών δεδομένων στο κεφάλαιο 72, υπό τον αντίστοιχο τίτλο (μεταφορές προσωπικών πληροφοριών εκτός της Δημοκρατίας)[469].

Σύμφωνα με τις διατάξεις του 72ου τμήματος του νόμου, οι εξαγωγές των προσωπικών δεδομένων εκτός της χώρας μπορούν να πραγματοποιούνται σε ορισμένες περιπτώσεις, οι οποίες αναλύονται εκτενώς. Ο πρώτος μηχανισμός, από τους πέντε που θεσπίζονται, αφορά την ύπαρξη δεσμευτικών εταιρικών κανόνων ή δεσμευτικής συμφωνίας. Εν συνεχεία, προβλέπεται ο διασυνοριακός μηχανισμός της συγκατάθεσης του υποκειμένου των δεδομένων.

Η διασυνοριακή μεταφορά των δεδομένων μπορεί επίσης να πραγματοποιηθεί όταν καθίσταται απαραίτητη για τη «σύναψη σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου μέρους», ή για το προσυμβατικό στάδιο.

Τέλος, η διασυνοριακή μεταφορά μπορεί να πραγματοποιηθεί, ούσα απαραίτητη για τη σύναψη ή την εκτέλεση μιας σύμβασης, «η οποία συνάπτεται προς το συμφέρον του υποκειμένου των δεδομένων μεταξύ του υπεύθυνου μέρους και τρίτου μέρους» και όταν η διαβίβαση είναι προς το όφελος του υποκειμένου των δεδομένων, στην περίπτωση κατά την οποία αφενός δεν καθίσταται εύλογα εφικτή η συγκατάθεση και αφετέρου, εάν ήταν εύλογα εφικτή, το υποκείμενο των δεδομένων πιθανώς θα την παρέχει.

Συνεπώς, μπορεί να εξαχθεί το συμπέρασμα ότι οι πέντε μηχανισμοί που διέπουν τις διασυνοριακές ροές των δεδομένων εμφανίζουν αρκετά κοινά σημεία τόσο με την προϊσχύουσα ευρωπαϊκή Οδηγία 95/46/ΕΚ[470], όσο και με τον ισχύοντα GDPR.

7.4 Ρυθμίσεις σε επιλεγμένες χώρες της Βορείου Αμερικής

7.4.1 Καναδάς

Ο Νόμος περί προστασίας προσωπικών πληροφοριών και ηλεκτρονικών εγγράφων (Personal Information Protection and Electronic Documents Act,

[469] Βλ. https://popia.co.za/section-72-transfers-of-personal-information-outside-republic/

[470] Makulilo, A. B. (Ed.). (2016). *African data privacy laws* (Vol. 33). Cham: Springer.

PIPEDA) του Καναδά του 2000[471] αντιμετωπίζει τη διασυνοριακή ροή των δεδομένων στο άρθρο 4.1.3 του Παραρτήματος Ι [472].

Ο Νόμος περί προστασίας προσωπικών πληροφοριών και ηλεκτρονικών εγγράφων, όπως ισχύει, επιτρέπει την εξαγωγή των προσωπικών δεδομένων σε μία οντότητα που βρίσκεται εκτός του Καναδά, ρίχνοντας όμως το βάρος στην υποχρέωση λογοδοσίας των εξαγωγέων[473]. Ειδικότερα, το άρθρο 4.1.3 αναδεικνύει την υποχρέωση της συνεχούς επίβλεψης της προστασίας των προσωπικών δεδομένων, ακόμη και μετά τη μεταφορά. Παράλληλα, ο τρόπος με τον οποίο θα επιτυγχάνεται η υποχρέωση λογοδοσίας των οργανισμών αναφέρεται στο δεύτερο εδάφιο του άρθρου. Αναλυτικότερα, προβλέπεται ότι η συνεχής προστασία των προσωπικών δεδομένων, στο πλαίσιο μίας διασυνοριακής διαβίβασης, εξασφαλίζεται με «συμβατικά ή άλλα μέσα για την παροχή συγκρίσιμου επιπέδου προστασίας κατά την επεξεργασία των πληροφοριών από το τρίτο μέρος»[474].

Κατά συνέπεια, ο Καναδάς, αν και έχει λάβει απόφαση επάρκειας[475] από την Ευρωπαϊκή Επιτροπή, αποδεικνύεται ότι έχει υιοθετήσει την προσέγγιση των διασυνοριακών ροών με κριτήριο τους οργανισμούς και όχι το γεωγραφικό κριτήριο, το οποίο βασίζεται κυρίως στην επάρκεια του μοντέλου της τρίτης χώρας[476]. Μάλιστα, η θέση αυτή διατυπώθηκε ρητά από την αρχή προστασίας των προσωπικών δεδομένων της χώρας[477].

---

[471] Βλ. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[472] Privacy Commissioner of Canada. (2009). Guidelines for Processing Personal Data Across Borders. Διαθέσιμο στο: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

[473] Scassa, T. (2020). Data Protection and the Internet: Canada. In *Data Protection in the Internet* (pp. 55-76). Springer, Cham.

[474] Personal Information Protection and Electronic Documents Act.

[475] 2002/2/ΕΚ: Απόφαση της Επιτροπής, της 20ής Δεκεμβρίου 2001, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα του καναδικού νόμου περί προστασίας των δεδομένων προσωπικού χαρακτήρα και ηλεκτρονικών εγγράφων.

[476] Privacy Commissioner of Canada. (2009). Guidelines for Processing Personal Data Across Borders. Διαθέσιμο στο: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

[477] Βλ. Privacy Commissioner of Canada. (2009). Guidelines for Processing Personal Data Across Borders. Διαθέσιμο στο: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

7.5 Ρυθμίσεις σε επιλεγμένες χώρες της Ευρώπης εκτός ΕΟΧ

7.5.1 Ρωσία

Ο ομοσπονδιακός νόμος της Ρωσίας N 152-FZ για τα προσωπικά δεδομένα της 27ης Ιουλίου 2006 (Federal Law of 27 July 2006 N 152-FZ ON PERSONAL DATA)[478] εμπεριέχει τη ρύθμιση των διασυνοριακών ροών των δεδομένων στο άρθρο 12 υπό τον αντίστοιχο τίτλο[479].

Αρχικά, θα πρέπει να αναφερθεί ότι το σύστημα των διασυνοριακών ροών των δεδομένων το οποίο έχει θέσει η Ρωσία έχει ως κεντρικό άξονα τη Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, καθότι αποτελεί μέλος του Συμβουλίου της Ευρώπης[480].

Αναλυτικότερα, το σύστημα παροχής επάρκειας των τρίτων χωρών, στο οποίο μπορεί να βασιστεί η διασυνοριακή ροή των δεδομένων, εκκινεί από την προσχώρηση στη Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα αλλά και από τους κανόνες που τίθενται σε αυτή. Πιο συγκεκριμένα, η παρ. 1 του άρθρου 12 του N 152-FZ καταρχήν επιτρέπει τη διαβίβαση προσωπικών δεδομένων σε τρίτα κράτη, είτε συμβαλλόμενα στη Σύμβαση του Συμβουλίου της Ευρώπης, είτε σε αυτά που παρέχουν επαρκές επίπεδο προστασίας των δεδομένων. Ωστόσο οι ροές δεδομένων «μπορούν να απαγορευτούν ή να περιοριστούν με σκοπό την προστασία των θεμελίων της συνταγματικής τάξης της Ρωσικής Ομοσπονδίας, της δημόσιας ηθικής και της υγείας, των δικαιωμάτων και των νόμιμων συμφερόντων των πολιτών και για την εθνική άμυνα και κρατική ασφάλεια».

Επιπλέον, η παρ. 2 του άρθρου 12 θέτει ως προϋπόθεση έγκρισης των τρίτων χωρών που δεν αποτελούν συμβαλλόμενα μέρη στη Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα τη συμμόρφωση με τις ρυθμίσεις της Σύμβασης.

Η παρ. 4 του άρθρου 12 ορίζει τους πέντε μηχανισμούς με τους οποίους μπορεί να πραγματοποιηθεί μία διασυνοριακή διαβίβαση σε τρίτο κράτος που δεν διαθέτει επαρκές επίπεδο προστασίας των δεδομένων. Τα εργαλεία περιλαμβάνουν συνοπτικά: «τη συγκατάθεση του υποκειμένου των δεδομένων,

[478] Βλ. https://pd.rkn.gov.ru/authority/p146/p164/

[479] Khorev, P., & Chernetsov, A. (2020). The Problem of Ensuring Cross-border Personal Data Transfer and Methods for Its Solving. In *2020 V International Conference on Information Technologies in Engineering Education (Inforino)* (pp. 1-4). IEEE.

[480] Βλ. https://www.coe.int/el/web/about-us/our-member-states

τις οριζόμενες σε συμφωνίες του κράτους περιπτώσεις, τις περιπτώσεις που προβλέπεται από ομοσπονδιακούς νόμους, την εκτέλεση μιας σύμβασης στην οποία είναι μέρος το υποκείμενο των προσωπικών δεδομένων, για τον σκοπό της προστασίας της ζωής, της υγείας και άλλων ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλων προσώπων, όταν είναι αδύνατο να ληφθεί η γραπτή συγκατάθεση του υποκειμένου των δεδομένων»[481].

7.6 Ρυθμίσεις σε επιλεγμένες χώρες της Νοτίου Αμερικής

7.6.1 Αργεντινή

Ο Νόμος 25.326 περί προστασίας των δεδομένων προσωπικού χαρακτήρα (Personal Data Protection Act)[482] της Αργεντινής, ο οποίος εκδόθηκε το 2000, περιλαμβάνει τους κύριους κανόνες που αφορούν την προστασία των προσωπικών δεδομένων στη χώρα[483]. Η διασυνοριακή ροή των προσωπικών δεδομένων προβλέπεται στο 12^{ο} κεφάλαιο του νόμου.

Καταρχάς, θα πρέπει να σημειωθεί ότι η παρ. 1 του 12^{ου} κεφαλαίου απαγορεύει τις διασυνοριακές ροές των δεδομένων σε χώρες οι οποίες δεν εξασφαλίζουν επαρκές επίπεδο προστασίας των δεδομένων και η παρ. 2 θέτει τις συγκεκριμένες πέντε περιπτώσεις κατά τις οποίες θα επιτρέπονται κατ' εξαίρεση[484]. Οι περιπτώσεις αυτές αφορούν: «διεθνή δικαστική συνεργασία, ανταλλαγή ιατρικών πληροφοριών, χρηματιστηριακές ή τραπεζικές διαβιβάσεις, διαβιβάσεις στο πλαίσιο διεθνών συνθηκών, στο πλαίσιο διεθνούς συνεργασίας μεταξύ υπηρεσιών πληροφοριών στον αγώνα κατά του οργανωμένου εγκλήματος, της τρομοκρατίας και της διακίνησης ναρκωτικών»[485].

Αξίζει να σημειωθεί ότι η Αργεντινή έλαβε την απόφαση επάρκειας από την Ευρωπαϊκή Επιτροπή[486] για το επίπεδο προστασίας των προσωπικών δεδομένων που διαθέτει, κατόπιν της έκδοσης αυτού του νόμου.

---

[481] Federal Law of 27 July 2006 N 152-FZ ON PERSONAL DATA.

[482] Βλ. http://www.jus.gob.ar/media/3201023/personal_data_protection_act25326.pdf

[483] Piper, D. L. A. (2021). *Data protection laws of the world: full handbook*. DLA Piper.

[484] PERSONAL DATA PROTECTION ACT 25.326.

[485] PERSONAL DATA PROTECTION ACT 25.326.

[486] 2003/490/ΕΚ: Απόφαση της Επιτροπής, της 30ής Ιουνίου 2003, δυνάμει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια προστασίας δεδομένων προσωπικού χαρακτήρα στην Αργεντινή.

7.6.2 Βραζιλία

Ο γενικός νόμος περί προστασίας των δεδομένων της Βραζιλίας no. 13,709/2018 (The Brazilian General Data Protection Law, LGPD), τέθηκε σε ισχύ στις 18 Σεπτεμβρίου 2020 και αποτελεί την πρώτη ολοκληρωμένη νομική ρύθμιση της χώρας για την προστασία των δεδομένων[487]. Η ρύθμιση της διασυνοριακής ροής των δεδομένων προβλέπεται στα άρθρα 33-35 του νόμου[488].

Ο γενικός νόμος περί προστασίας δεδομένων της Βραζιλίας επιτρέπει τη διασυνοριακή ροή προσωπικών δεδομένων σε χώρες που παρέχουν επαρκές επίπεδο προστασίας των προσωπικών δεδομένων και όταν υφίστανται: συμβατικές ρήτρες για την εκάστοτε διαβίβαση, τυποποιημένες συμβατικές ρήτρες, παγκόσμιοι εταιρικοί κανόνες και έγκυρα αποδεικτικά ποιότητας/πιστοποιητικά/κώδικες δεοντολογίας[489]. Από τα προαναφερθέντα, συνάγεται η αντιστοιχία των εν λόγω ρυθμίσεων με τον GDPR.

Επιπρόσθετα, περαιτέρω νομικές βάσεις της διαβίβασης δεδομένων σε τρίτες χώρες του γενικού νόμου περί προστασίας των δεδομένων no. 13,709/2018 αποτελούν οι εξής περιπτώσεις: όταν η διαβίβαση είναι απαραίτητη για τη διεθνή νομική συνεργασία μεταξύ των αρχών επιβολής του νόμου, σύμφωνα με το διεθνές δίκαιο, όταν η διαβίβαση είναι απαραίτητη για την προστασία της ζωής ή της φυσικής ασφάλειας του υποκειμένου των δεδομένων ή τρίτου μέρους, όταν έχει δοθεί από το υποκείμενο των δεδομένων μία κατ' εξαίρεση συγκατάθεση για τη συγκεκριμένη διαβίβαση, όταν η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης ή του προσυμβατικού σταδίου, όταν η διαβίβαση είναι απαραίτητη για την άσκηση δικαιωμάτων στο πλαίσιο δικαστικών, διοικητικών ή διαιτητικών διαδικασιών, και τέλος, όταν η διαβίβαση είναι απαραίτητη για την άσκηση δημόσιας εξουσίας ή νομικού καταλογισμού των δημοσίων υπηρεσιών[490].

[487] Piper, D. L. A. (2021). *Data protection laws of the world: full handbook*. DLA Piper.

[488] OneTrust DataGuidance, Baptista Luz Advogados. (2020). Comparing privacy laws: GDPR v. LGPD.

[489] OneTrust DataGuidance, Baptista Luz Advogados. (2020). Comparing privacy laws: GDPR v. LGPD.

[490] OneTrust DataGuidance, Baptista Luz Advogados. (2020). Comparing privacy laws: GDPR v. LGPD.

7.7 Ρυθμίσεις σε επιλεγμένες χώρες της Ωκεανίας

7.7.1 Αυστραλία

Ο αυστραλιανός νόμος περί απορρήτου του 1988 (Privacy Act 1988), όπως ισχύει[491], συνιστά την κύρια νομοθεσία όσον αφορά την προστασία των προσωπικών δεδομένων στη χώρα[492].

Η διασυνοριακή ροή των προσωπικών δεδομένων από την Αυστραλία σε τρίτες χώρες προβλέπεται στην 8η αρχή του νόμου περί απορρήτου του 1988 με τίτλο: «Διασυνοριακή αποκάλυψη προσωπικών πληροφοριών». Καταρχήν, θα πρέπει να αναφερθεί ότι στην παράγραφο 8.1 τίθεται το γενικό πλαίσιο που διέπει τις διαβιβάσεις σε τρίτες χώρες, όπου οι εξαγωγείς μπορεί να είναι άτομα ή οικονομικές οντότητες. Πιο συγκεκριμένα, θεσπίζεται ότι πρέπει να λαμβάνονται τα κατάλληλα μέτρα που να διασφαλίζουν ότι ο εισαγωγέας των δεδομένων στην τρίτη χώρα δεν παραβιάζει τις αυστραλιανές αρχές προστασίας των προσωπικών δεδομένων[493].

Επιπλέον, σύμφωνα με την παράγραφο 2, η διασυνοριακή διαβίβαση δύναται να πραγματοποιηθεί όταν ο εισαγωγέας των δεδομένων: «υπόκειται σε νόμο ή συμβατική δέσμευση, που έχουν ως αποτέλεσμα την προστασία των πληροφοριών με τρόπο που θα είναι, σε γενικές γραμμές, τουλάχιστον αντίστοιχος κατ' ουσία με τον τρόπο που προστατεύουν οι αρχές της Αυστραλίας τις πληροφορίες και υφίστανται μηχανισμοί στους οποίους μπορεί να έχει πρόσβαση το άτομο για να λάβει μέτρα για την επιβολή αυτής της προστασίας του νόμου ή της συμβατικής δέσμευσης».

Παράλληλα, η διαβίβαση μπορεί να στηρίζεται στη συγκατάθεση του υποκειμένου των δεδομένων, με την επιφύλαξη ότι το άτομο έχει προηγουμένως ενημερωθεί ότι η παροχή της συγκατάθεσής του σηματοδοτεί την απαλλαγή της υποχρέωσης της οντότητας να λάβει εύλογα μέτρα για να διασφαλίσει ότι ο εισαγωγέας των δεδομένων δεν παραβιάζει τις αρχές του αυστραλιανού νόμου.

Επιπρόσθετα, μία διασυνοριακή διαβίβαση δύναται να πραγματοποιηθεί είτε όταν απαιτείται ή επιτρέπεται από τους αυστραλιανούς νόμους ή τις αυστραλιανές δικαστικές αποφάσεις είτε στην περίπτωση που υφίσταται μία γενική άδεια για αυτήν. Μία οντότητα, ακόμη, μπορεί να εισάγει δεδομένα σε τρίτη χώρα, όταν αυτό προβλέπεται σε διεθνή συμφωνία.

Τέλος, η διασυνοριακή διαβίβαση μπορεί να βασίζεται στο γεγονός ότι καθίσταται αφενός αναγκαία σε δραστηριότητες επιβολής (όπως αυτές ορίζονται

[491] Βλ. https://www.legislation.gov.au/Details/C2014C00076

[492] Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature, p 115.

[493] Privacy Act 1988, παρ 8.1.

στο Τμήμα 1-Γενικοί ορισμοί του 2ου μέρους του νόμου) που διεξάγονται από/ή για λογαριασμό του φορέα επιβολής και αφετέρου ο εισαγωγέας των δεδομένων «είναι φορέας που εκτελεί λειτουργίες ή ασκεί εξουσίες, αντίστοιχες με εκείνες που εκτελούνται ή ασκούνται από έναν φορέα επιβολής» [494].

7.7.2 Νέα Ζηλανδία

Ο νόμος της Νέας Ζηλανδίας περί απορρήτου του 2020 (Privacy Act 2020) τέθηκε σε ισχύ την 1η Δεκεμβρίου 2020, αντικαθιστώντας τον προϊσχύοντα νόμο περί απορρήτου του 1993[495]. Η αντιμετώπιση των διασυνοριακών ροών των προσωπικών δεδομένων περιλαμβάνεται στη 12η αρχή του απορρήτου των πληροφοριών στο 3ο τμήμα του ιδιαίτερα αναλυτικού νόμου[496].

Πιο συγκεκριμένα, η 12η αρχή αναφέρει ότι η διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες επιτρέπεται, εν πρώτοις, όταν ο εισαγωγέας των δεδομένων υπόκειται στον νόμο περί απορρήτου της Νέας Ζηλανδίας, λόγω της δραστηριοποίησής του στη χώρα. Επιπλέον, η διαβίβαση επιτρέπεται όταν ο εισαγωγέας των δεδομένων υπόκειται σε νομοθεσία, η οποία παρέχει αντίστοιχες εγγυήσεις για την προστασία της ιδιωτικότητας με τον νόμο περί απορρήτου του 2020 ή έχει συμφωνήσει στην επαρκή προστασία των προσωπικών δεδομένων. Παράλληλα, η διαβίβαση δύναται να πραγματοποιηθεί μέσω ενός δεσμευτικού συστήματος ή όταν ο εισαγωγέας υπόκειται στη νομοθεσία των χωρών που έχει προκαθορίσει η Νέα Ζηλανδία. Τέλος, η διασυνοριακή διαβίβαση μπορεί να βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων[497] [498].

[494] Privacy Act 1988, παρ. 8.2.

[495] https://www.privacy.org.nz/privacy-act-2020/privacy-act-2020/

[496] Βλ. https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23376

[497] Office of the Privacy Commissioner. (2021). A quick tour of the privacy principles. Διαθέσιμο στο: https://www.privacy.org.nz/privacy-act-2020/privacy-principles/the-privacy-principles/

[498] Βλ. https://www.privacy.org.nz/privacy-act-2020/privacy-principles/12/

ΚΕΦΑΛΑΙΟ 8. ΟΙ ΡΥΘΜΙΣΕΙΣ ΤΗΣ ΔΙΑΣΥΝΟΡΙΑΚΗΣ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ ΣΕ ΕΝΩΣΙΑΚΟ ΕΠΙΠΕΔΟ

8.1 Εισαγωγή

Στο παρόν κεφάλαιο πραγματοποιείται η ανάλυση των ρυθμίσεων του ενωσιακού δικαίου που αφορούν τη διασυνοριακή ροή των προσωπικών δεδομένων. Η παρουσίαση των νομοθετικών κειμένων αποτυπώνεται από το παλαιότερο στο νεότερο προκειμένου να αντανακλάται η διαχρονική πορεία του δικαίου των προσωπικών δεδομένων. Οι νομοθετικές ρυθμίσεις του παρόντος κεφαλαίου δύνανται να επηρεάσουν ή έχουν ως αντικείμενο την προστασία των προσωπικών δεδομένων. Τις κεντρικότερες για το δίκαιο των προσωπικών δεδομένων και ως εκ τούτου για τη ρύθμιση της διασυνοριακής ροής των οικονομικών δεδομένων, βάσει αντικειμένου, αποτελούν η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

8.2 Η σύμβαση εφαρμογής της συμφωνίας του Σένγκεν και το σύστημα πληροφοριών Σένγκεν (SIS και SSI II)

Η συμφωνία του Σένγκεν υπογράφθηκε στις 14 Ιουνίου 1985 μεταξύ του Βελγίου, της Γαλλίας, της Γερμανίας, της Ολλανδίας και του Λουξεμβούργου. Αντικείμενο της συμφωνίας αποτέλεσε η κατάργηση των ελέγχων στα εσωτερικά σύνορά τους καθώς και η θέσπιση του καθεστώτος ελεύθερης κυκλοφορίας όλων των υπηκόων των χωρών, οι οποίες την έχουν υπογράψει[499]. Η σύμβαση Σένγκεν υπογράφθηκε από τις ίδιες χώρες στις 19 Ιουνίου 1990 και τέθηκε σε ισχύ το 1995, προβλέποντας τις προϋποθέσεις εφαρμογής της συμφωνίας του Σένγκεν[500]. Το «κεκτημένο Σένγκεν» εντάχθηκε στην ενωσιακή νομοθεσία το 1999 με τη συνθήκη του Άμστερνταμ[501].

Ο χώρος Σένγκεν απαρτίζεται σήμερα από 26 ευρωπαϊκές χώρες[502], συμπεριλαμβανομένων 22 εκ των 27 κρατών μελών της ΕΕ. Η Ιρλανδία είναι το

[499] Βλ. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:schengen_agreement

[500] Βλ. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:schengen_agreement

[501] Ψαρογίαννη, Σ. (2010). Η διασυνοριακή ροη πληροφοριών στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας και η προστασία των δεδομένων προσωπικού χαρακτήρα, σελ. 9 κ. επ.

[502] Στο χώρο Σένγκεν μετέχουν: Αυστρία, Βέλγιο, Τσεχία, Δανία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ισλανδία, Ιταλία, Λετονία, Λιχτενστάιν, Λιθουανία, Λουξεμβούργο, Μάλτα, Ολλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Σλοβακία, Σλοβενία, Ισπανία , Σουηδία και Ελβετία.

μόνο κράτος μέλος της ΕΕ που δε συμμετέχει στον χώρο Σένγκεν. Για την ακρίβεια, η Ιρλανδία δεν συμμετέχει στον χώρο Σένγκεν, ενώ η Βουλγαρία, η Κροατία, η Κύπρος και η Ρουμανία μετέχουν με εδικό καθεστώς[503].

Το Σύστημα Πληροφοριών Schengen (Schengen Information System, SIS), του οποίου η δημιουργία θεσπίζεται στο άρθρο 92 της Σύμβασης εφαρμογής της συμφωνίας του Σένγκεν[504], είναι ένα κοινό ηλεκτρονικό αρχείο δεδομένων, το οποίο τα κράτη μέλη τροφοδοτούν με δεδομένα υπό τις προϋποθέσεις του άρθρου 94. Η πρώτη κατηγορία πληροφοριών αφορά πρόσωπα (διωκόμενοι, εξαφανισμένοι ενήλικες και ανήλικοι κ.λπ.) και η δεύτερη περιλαμβάνει αναζητούμενα οχήματα ή αντικείμενα, όπως έγγραφα ταυτότητας, άδειες κυκλοφορίας οχημάτων και πινακίδες αριθμού κυκλοφορίας που έχουν κλαπεί ή απολεσθεί[505].

Στο κεφάλαιο 3 (άρθρα 102-118) της Σύμβασης εφαρμογής της συμφωνίας του Σένγκεν περιγράφεται η «Προστασία των δεδομένων προσωπικού χαρακτήρα και ασφάλεια των δεδομένων στα πλαίσια του συστήματος πληροφοριών Σένγκεν». Ως προς το πεδίο της διαβίβασης προσωπικών δεδομένων, οι παράγραφοι 1 και 2 του άρθρου 117 της Σύμβασης αναφέρονται στις προϋποθέσεις διαβίβασης προσωπικών δεδομένων στο έδαφος των συμβαλλόμενων μερών. Αναλυτικότερα, η διαβίβαση ερείδεται, κατά την παρ. 1, στο αντίστοιχο επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα «προς αυτό που απορρέει από τις αρχές της Σύμβασης του Συμβουλίου της Ευρώπης, της 28ης Ιανουαρίου 1981 για την προστασία των ατόμων έναντι της αυτόματης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και της σύστασης R (87) 15, της 17ης Σεπτεμβρίου 1987, της επιτροπής υπουργών του Συμβουλίου της Ευρώπης». Παράλληλα, ο τίτλος VI θεσπίζει στο άρθρο 126 την προστασία δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται κατ' εφαρμογή της Σύμβασης με σημείο αναφοράς τη Σύμβαση του Συμβουλίου της Ευρώπης

[503]Βλ. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:schengen_agreement

[504]Σύμβαση εφαρμογής της συμφωνίας του Σένγκεν της 14ης Ιουνίου 1985 μεταξύ των κυβερνήσεων των κρατών της Οικονομικής Ένωσης Μπενελούξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας, σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A42000A0922%2802%29

[505]http://www.hellenicpolice.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=26982&Itemid=898&lang

του 1981 και τη σύσταση R (87) 15 της επιτροπής υπουργών του Συμβουλίου της Ευρώπης[506].

Το Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς (Schengen Information System, II, SIS II) έχει τεθεί σε εφαρμογή από τις 9 Απριλίου 2013 με την Απόφαση 2013/157/ΔΕΥ[507] του Συμβουλίου[508], έχοντας ως νομικές βάσεις την Απόφαση 2007/533/ΔΕΥ[509] και τον Κανονισμό 1987/2006 (SIS II)[510] [511].

Ειδικότερα, θα πρέπει να αναφερθεί ότι ο Κανονισμός 1987/2006 στο άρθρο 39 απαγορεύει τη διαβίβαση των επεξεργαζόμενων δεδομένων στο πλαίσιο του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς σε τρίτες χώρες ή διεθνείς οργανισμούς. Παράλληλα, στο άρθρο 44, ο Κανονισμός 1987/2006 αναθέτει στις εθνικές εποπτικές αρχές προστασίας των δεδομένων τον έλεγχο της νομιμότητας της επεξεργασίας των προσωπικών δεδομένων του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς στο «έδαφος του κράτους στο οποίο υπάγονται και τη διαβίβασή τους από το έδαφος αυτό, καθώς και ως προς την ανταλλαγή και περαιτέρω επεξεργασία συμπληρωματικών πληροφοριών». Επιπλέον, θα πρέπει να σημειωθεί ότι ο Κανονισμός 1987/2006 απαγορεύει την επεξεργασία ειδικών κατηγοριών «ευαίσθητων» προσωπικών δεδομένων στο πλαίσιο του Συστήματος.

Κύριο ζήτημα, ως προς την προστασία των προσωπικών δεδομένων, αποτελεί η διευκρίνιση του νομικού εργαλείου που διέπει το Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς. Η Απόφαση 2007/533/ΔΕΥ στο άρθρο 57 θέτει ως έρεισμα της νόμιμης επεξεργασίας των προσωπικών δεδομένων τη

---

[506]Βλ. Μεταξάκης, Ε. (2014). Η διακρατική ηλεκτρονική ροή ευαίσθητων προσωπικών δεδομένων – Το ρυάκι που έγινε χείμαρρος. *ΔΙΜΕΕ, 2*, 170-178.

[507] 2013/157/ΕΕ: Απόφαση του Συμβουλίου, της 7ης Μαρτίου 2013, που ορίζει την ημερομηνία εφαρμογής της απόφασης 2007/533/ΔΕΥ σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32013D0157

[508]Βλ.https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/megales_baseisdedomenon/SISII

[509] Απόφαση 2007/533/ΔΕΥ του Συμβουλίου, της 12ης Ιουνίου 2007, σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32007D0533.

[510] Κανονισμός (ΕΚ) αριθ. 1987/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Δεκεμβρίου 2006, σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32006R1987

[511] Ψαρογίαννη, Σ. (2010). Η διασυνοριακή ροη πληροφοριών στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας και η προστασία των δεδομένων προσωπικού χαρακτήρα, σελ. 9 κ. επ.

Σύμβαση του Συμβουλίου της Ευρώπης της 28ης Ιανουαρίου 1981 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα με τις τροποποιήσεις της[512], το οποίο έρχεται σε αντιστοιχία με το γεγονός ότι όλα τα κράτη που ανήκουν στο Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς είναι και συμβαλλόμενα μέρη της Σύμβασης 108/1981[513]. Ωστόσο, όπως υποστηρίζεται[514], οι διατάξεις του Κανονισμού 1987/2006 για την προστασία των προσωπικών δεδομένων, ισχύουν ως ειδικότερες της Σύμβασης 108/1981 και του GDPR.

Επιπρόσθετα, ως προς το ζήτημα της εφαρμογής του GDPR, δεν πρέπει να παραλειφθεί το γεγονός ότι τα κράτη που ανήκουν στον χώρο Σένγκεν ανήκουν στον ΕΟΧ, στον οποίο ισχύει ο GDPR[515], με μόνη εξαίρεση την Ελβετία που δεν ανήκει στον ΕΟΧ. Το γεγονός αυτό συνεπάγεται ότι οι χώρες του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς, οι οποίες βρίσκονται υπό την εμβέλεια του GDPR, αφενός έχουν το ίδιο επίπεδο προστασίας για τα προσωπικά δεδομένα και αφετέρου μεταξύ τους δεν υφίσταται η έννοια της διασυνοριακής ροής δεδομένων προς τρίτες χώρες.

Όσον αφορά την περίπτωση της Ελβετίας ως μέλος του Σενγκεν, ο GDPR θεσπίζει την εξωεδαφική εφαρμογή του όταν τα δεδομένα του Συστήματος ανήκουν σε υποκείμενα που βρίσκονται εντός της ΕΕ (άρθρο 3 παρ. 2 GDPR). Αυτό συνεπάγεται ότι ο GDPR ισχύει σε επεξεργασίες δεδομένων που διενεργούνται στην Ελβετία στο πλαίσιο του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς σε ότι αφορά δεδομένα ατόμων που βρίσκονται στην ΕΕ. Παράλληλα, θα πρέπει να αναφερθεί ότι η Ελβετία έχει λάβει απόφαση

[512] Βλ. Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 392.

[513] Majcher, I. (2020). The Schengen-wide entry ban: how are non-citizens' personal data protected?. *Journal of Ethnic and Migration Studies*, 1-17.

[514] Majcher, I. (2020). The Schengen-wide entry ban: how are non-citizens' personal data protected?. *Journal of Ethnic and Migration Studies*, 1-17.

[515] Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]. Διαθέσιμο στο: https://www.efta.int/sites/default/files/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20English/154-2018.pdf

επάρκειας[516] από την Ευρωπαϊκή Επιτροπή, η οποία αναγνώρισε με αυτόν τον τρόπο το επίπεδο προστασίας των δεδομένων της χώρας ως αντίστοιχο της ΕΕ.

8.3 Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Η Οδηγία 95/46/ΕΚ[517] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία έχει αντικατασταθεί από τον GDPR, αποτελεί σημείο αναφοράς για το δίκαιο των προσωπικών δεδομένων στον ευρωπαϊκό χώρο[518] [519] [520]. Η Οδηγία στόχευσε στην εναρμόνιση των εθνικών νομοθεσιών των ευρωπαϊκών κρατών ως προς την προστασία των προσωπικών δεδομένων[521], μέσω της υποχρέωσης μεταφοράς της στο εσωτερικό δίκαιο των κρατών[522]. Ειδικότερα, στο πεδίο της διασυνοριακής διαβίβασης των προσωπικών δεδομένων, θα πρέπει να σημειωθεί ότι η Οδηγία 95/46/ΕΚ ίσχυε στον ΕΟΧ[523], ο οποίος περιλαμβάνει τα κράτη μέλη της ΕΕ και την Ισλανδία, Λιχτενστάιν και Νορβηγία[524]. Επομένως, οι υπόλοιπες χώρες νοούνται ως τρίτες χώρες για τη διαβίβαση των προσωπικών δεδομένων σε αυτές.

---

[516] 2000/518/ΕΚ: Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, δυνάμει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα που παρέχεται στην Ελβετία. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32000D0518

[517] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A31995L0046

[518] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 207 κ. επ.

[519] Βλ. Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (νέο δίκαιο-νέες υποχρεώσεις-νέα δικαιώματα)*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 11 κ. επ.

[520] Βλ. Τζωρτζάτου, Ο. (2015). *Η προστασία των ευαίσθητων προσωπικών δεδομένων της υγείας στη βιοϊατρική έρευνα*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 26 κ. επ.

[521] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 207 κ. επ.

[522] Σαχπεκίδου, Ε. Ρ. (2011). *Ευρωπαϊκό Δίκαιο*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 461.

[523] Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication Services) to the EEA Agreement. Διαθέσιμο στο: https://www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/1999%20-%20English/083-1999.pdf

[524] Βλ. https://www.efta.int/eea

Ωστόσο, πριν την ανάλυση των σχετικών με τη διασυνοριακή ροή των προσωπικών δεδομένων άρθρων της Οδηγίας 95/46/ΕΚ, κρίνεται αξιοσημείωτη η αποσαφήνιση του όρου της διασυνοριακής ροής σε τρίτες χώρες υπό το πρίσμα του Ευρωπαϊκού Δικαστηρίου, δεδομένου ότι η Οδηγία δεν περιλαμβάνει ορισμό της έννοιας[525]. Πιο συγκεκριμένα, το πέμπτο προδικαστικό ερώτημα της υπόθεσης C-101/01[526] [527] αφορούσε την εξέταση της ερμηνείας της «διαβίβασης δεδομένων προς τρίτη χώρα», σύμφωνα με το άρθρο 25 της Οδηγίας 95/46/ΕΚ. Ειδικότερα, το ζήτημα που εξετάστηκε αναφερόταν στο κατά πόσο υφίσταται διασυνοριακή διαβίβαση σε τρίτη χώρα όταν ένα πρόσωπο που βρίσκεται εντός κράτους μέλους αναγράφει σε ιστοσελίδα του Διαδικτύου προσωπικά δεδομένα, καθιστώντας δυνατή την πρόσβαση σε άτομα εγκατεστημένα σε τρίτες χώρες[528]. Καταρχάς, θα πρέπει να αναφερθεί ότι κατ' ουσία το ερώτημα που τέθηκε στο Δικαστήριο ήταν αν η ανάρτηση προσωπικών δεδομένων στο Διαδίκτυο συνιστά διασυνοριακή διαβίβαση των δεδομένων. Η απάντηση του Δικαστηρίου επικεντρώθηκε στο γεγονός ότι αν ταύτιζε την έννοια της ανάρτησης στο Διαδίκτυο με τη διασυνοριακή διαβίβαση σε τρίτες χώρες, τότε αφενός οι διασυνοριακοί μηχανισμοί των άρθρων 25 και 26 της Οδηγίας 95/46/ΕΚ θα έβρισκαν εφαρμογή σε όλες σχεδόν τις επεξεργασίες δεδομένων στο Διαδίκτυο και αφετέρου τα κράτη-μέλη θα υποχρεούνταν να εμποδίζουν έναν μεγάλο αριθμό διαβιβάσεων[529]. Συνεπώς, η απόφαση του Δικαστηρίου ήταν αρνητική ως προς τη διεύρυνση της έννοιας της διασυνοριακής ροής των προσωπικών δεδομένων, οριοθετώντας την εμβέλειά της, σε σχέση με το Διαδίκτυο, καταλυτικό παράγοντα για τα δεδομένα, το οποίο έκτοτε έχει αναπτυχθεί ακόμα περισσότερο.

Η διασυνοριακή ροή των προσωπικών δεδομένων εντοπίζεται στην Οδηγία 95/46/ΕΚ στα εξής σημεία: άρθρο 1 παρ. 2 και άρθρα 25-26[530]. Όσον αφορά τη διασυνοριακή ροή των προσωπικών δεδομένων μεταξύ των χωρών του ΕΟΧ, αυτή καθίσταται ελεύθερη από το άρθρο 1 της Οδηγίας 95/46/ΕΚ. Αντίθετα, η διαβίβαση των προσωπικών δεδομένων επιτρεπόταν, βάσει της

[525] C-101/01. Απόφαση του ΔΕΚ της 6ης Νοεμβρίου 2003, Ποινική δίκη κατά Bodil Lindqvist, Σκέψη 56.

[526] C-101/01. Απόφαση του ΔΕΚ της 6ης Νοεμβρίου 2003, Ποινική δίκη κατά Bodil Lindqvist.

[527]Βλ. Ιγγλεζάκης, Ι. (2003). ΔΕΚ της 6.11.2003, C-101/01, Gota Hovratt – Bodil Lindqvist. *Επισκόπηση Εμπορικού Δικαίου, 4,* 1041-1051.

[528] C-101/01. Απόφαση του ΔΕΚ της 6ης Νοεμβρίου 2003, Ποινική δίκη κατά Bodil Lindqvist, Σκέψη 52.

[529] C-101/01. Απόφαση του ΔΕΚ της 6ης Νοεμβρίου 2003, Ποινική δίκη κατά Bodil Lindqvist, Σκέψη 69.

[530] Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, pp. 40-46.

Οδηγίας 95/46/ΕΚ, όταν η τρίτη χώρα εισαγωγής των δεδομένων «εξασφαλίζει ικανοποιητικό επίπεδο προστασίας» (άρθρο 25 παρ. 1)[531] [532]. Οι χώρες, οι οποίες έχουν λάβει σύμφωνα με την Οδηγία 95/46/ΕΚ αποφάσεις επάρκειας (οι οποίες ισχύουν και επί του παρόντος) για τη διασυνοριακή ροή των δεδομένων σε αυτές, είναι οι εξής: Ανδόρα, Αργεντινή, Καναδάς, Φερόες Νήσοι, Γκέρνσεϊ, Ισραήλ, Νήσος του Μαν, Τζέρσεϊ, Νέα Ζηλανδία, Ελβετία, Ουρουγουάη[533]. Στην παρακάτω ενότητα (8.6.2.1) παρουσιάζονται όλες οι ισχύουσες αποφάσεις της Ευρωπαϊκής Επιτροπής, τόσο δυνάμει της Οδηγίας 95/46/ΕΚ όσο και δυνάμει του GDPR.

Όταν δεν υφίσταται απόφαση επάρκειας, μία εξαγωγή προσωπικών δεδομένων σε τρίτη χώρα, βάσει των θεσπιζόμενων στην Οδηγία 95/46/ΕΚ, εξεταζόταν κατά κύριο λόγο μεμονωμένα και κατά περίπτωση. Αναλυτικότερα, σύμφωνα με το άρθρο 26 παρ. 1, μία διαβίβαση των προσωπικών δεδομένων μπορούσε να βασίζεται σε μία από τις 6 περιπτώσεις/παρεκκλίσεις της παρ. 1 ως ακολούθως:

α) Ρητή συγκατάθεση του υποκειμένου των δεδομένων

β) Εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας ή «για την εκτέλεση προσυμβατικών μέτρων ληφθέντων κατ' αίτηση του προσώπου αυτού»

γ) Συνομολόγηση ή εκτέλεση σύμβασης «που έχει συναφθεί ή πρόκειται να συναφθεί μεταξύ του υπευθύνου επεξεργασίας και τρίτου προς το συμφέρον του προσώπου στο οποίο αναφέρονται τα δεδομένα»

δ) «Είναι αναγκαία ή απαιτείται εκ του νόμου για τη διασφάλιση σημαντικού δημοσίου συμφέροντος ή για την αναγνώριση, άσκηση ή υπεράσπιση ενός δικαιώματος ενώπιον του δικαστηρίου»

ε) «Είναι αναγκαία για τη διασφάλιση ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα»

[531] Βλ. Γιαννόπουλος, Γ. (2001). Προστασία προσωπικών δεδομένων και διασυνοριακή ροή πληροφοριών. Το πρόβλημα του «ικανοποιητικού επιπέδου προστασίας». *ΔτΑ*, 5, 733 κ. επ.

[532] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 119 κ. επ.

[533] European Commission. Adequacy decisions. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

στ) «Πραγματοποιείται από δημόσιο μητρώο το οποίο προορίζεται βάσει νομοθετικών ή κανονιστικών διατάξεων για την παροχή πληροφοριών στο κοινό και είναι προσιτό είτε στο κοινό γενικά είτε σε οποιοδήποτε πρόσωπο μπορεί να αποδείξει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι σχετικές νόμιμες προϋποθέσεις»

Υπό το πλαίσιο των παρεκκλίσεων του άρθρου 26 της Οδηγίας 95/46/ΕΚ, αξίζει να αναφερθεί ότι, σύμφωνα με την Ομάδα εργασίας του άρθρου 29[534], ο εισαγωγέας των προσωπικών δεδομένων στην τρίτη χώρα δεν απαιτείται να συμμορφώνεται με το επίπεδο προστασίας των δεδομένων που θεσπίζεται στην Οδηγία 95/46/ΕΚ για την επεξεργασία των δεδομένων στη χώρα του (π.χ. αρχές της σκοπιμότητας, ασφάλειας, δικαίωμα πρόσβασης κλπ.). Επιβεβαιώνεται, λοιπόν, ο ad hoc χαρακτήρας των παρεκκλίσεων, οι οποίες δεν είχαν τη μορφή του πάγιου κανόνα αλλά της κατ' εξαίρεση νόμιμης βάσης.

Παράλληλα, μία ή περισσότερες διαβιβάσεις μπορούσαν να πραγματοποιούνται βάσει επαρκών εγγυήσεων (όπως οι συμβατικές ρήτρες) του υπεύθυνου της επεξεργασίας «για την προστασία της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων καθώς και την άσκηση των σχετικών δικαιωμάτων». Ο εν λόγω μηχανισμός της παρ. 2 του άρθρου 26, ο οποίος ήταν και ιδιαίτερα συνήθης στην πράξη, εγκρινόταν από την αρχή προστασίας δεδομένων των κρατών-μελών[535], εκτός και αν είχε εγκριθεί από την Ευρωπαϊκή Επιτροπή βάσει της παρ. 4 του άρθρου 26 της Οδηγίας 95/46/ΕΚ[536]. Θα πρέπει να σημειωθεί ότι στο πλαίσιο αυτού του εργαλείου εντασσόταν ο μηχανισμός διαβίβασης των δεσμευτικών εταιρικών κανόνων[537] [538].

---

[534] Ομάδα εργασίας του άρθρου 29. (2005). «Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995». Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_el.pdf

[535] Βλαχόπουλος, Σ. (2018). Διασυνοριακή μεταβίβαση δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση προς τρίτες χώρες: Οι τελευταίες εξελίξεις, Πρακτικά Ημερίδας «Προστασία των δεδομένων προσωπικού χαρακτήρα», Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, 18 Σεπτεμβρίου 2017, Επιμέλεια: Τζώρτζη, Β., εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 29 κ. επ.

[536] Βλ. Ν. 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) άρθρο 9 παρ. 2 περ. στ. (ΦΕΚ Α΄50/10-4-1997).

[537] Ομάδα εργασίας του άρθρου 29. (2005). «Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995». Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_el.pdf

Συμπερασματικά, δύναται να αναφερθεί ότι οι μηχανισμοί της Οδηγίας 95/46/ΕΚ ως προς τη διασυνοριακή ροή των προσωπικών δεδομένων σε τρίτες χώρες έθεσαν τα θεμέλια προκειμένου οι χώρες εκτός ΕΕ, που επιθυμούν να συνεργάζονται κυρίως σε οικονομικό επίπεδο με την Ένωση, να υιοθετήσουν τους αντίστοιχους μηχανισμούς[539]. Παράλληλα, ακόμη και στην περίπτωση των κρατών που δεν θέσπισαν παρόμοια εργαλεία, θα μπορούσε να αναφερθεί ότι η ευρωπαϊκή Οδηγία 95/46/ΕΚ υποχρέωσε τους εισαγωγείς των δεδομένων στα τρίτα κράτη (ειδικότερα σε αυτά που δεν είχαν λάβει απόφαση επάρκειας) να εστιάσουν σε αυτά και να τα λαμβάνουν υπόψη σε κάθε διαβίβαση προσωπικών δεδομένων.

8.3.1 Ο ελληνικός νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Ο Ν. 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) μετέφερε στο εθνικό δίκαιο της Ελλάδας την Οδηγία 95/46/ΕΚ. Ο Ν. 2472/1997 έχει καταργηθεί εκτός των διατάξεων που αναφέρονται ρητά στο άρθρο 84 του Ν. 4624/2019[540]. Στην παρούσα ενότητα θα αναλυθεί το προϊσχύον πλαίσιο του Ν. 2472/1997 για τη διασυνοριακή ροή των δεδομένων σε σχέση με τους μηχανισμούς που αναφέρει η προϊσχύουσα Οδηγία 95/46/ΕΚ. Βέβαια, στο σημείο αυτό θα πρέπει να αναφερθεί ότι το πλαίσιο ασφαλώς είναι εν γένει ίδιο με την Οδηγία 95/46/ΕΚ[541] [542], διαθέτει όμως κάποιες εξειδικεύσεις και νομικές επιλογές στις οποίες αξίζει να γίνει αναφορά.

Αναλυτικότερα, το άρθρο 9 του Ν. 2472/1997, το οποίο έχει καταργηθεί, αναφέρεται στα εργαλεία διαβίβασης των προσωπικών δεδομένων. Καταρχάς, θα πρέπει να επισημανθεί ότι η ελεύθερη κυκλοφορία των δεδομένων μεταξύ των

---

[538] Article 29 Working Party. (2003). "Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers". Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

[539] Jougleux, P. (2016). *Ευρωπαϊκό Δίκαιο του Διαδικτύου*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 224.

[540] Βλ. https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpika

[541] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 123.

[542] Βλ. Βλαχόπουλος, Σ. (2018). Διασυνοριακή μεταβίβαση δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση προς τρίτες χώρες: Οι τελευταίες εξελίξεις, Πρακτικά Ημερίδας «Προστασία των δεδομένων προσωπικού χαρακτήρα», Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, 18 Σεπτεμβρίου 2017, Επιμέλεια: Τζώρτζη, Β., εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 29 κ. επ.

χωρών του ΕΟΧ (άρθρο 1 παρ. 2 της Οδηγίας 95/46/ΕΚ) έχει συμπεριληφθεί στο άρθρο 9 παρ. 1 περ. α του ελληνικού νόμου, όπως και οι παρεκκλίσεις του άρθρου 26 της Οδηγίας 95/46/ΕΚ, συγκεντρώνοντας έτσι τις διατάξεις που αφορούν τη διαβίβαση των προσωπικών δεδομένων σε ένα άρθρο. Η διαβίβαση των δεδομένων επιτρέπεται, σύμφωνα με το άρθρο 9 παρ. 1 περ. β του Ν. 2472/1997, κατόπιν άδειας της Αρχής προστασίας προσωπικών δεδομένων αφού κρίνει ως «ικανοποιητικό» το επίπεδο προστασίας της τρίτης χώρας ή κατόπιν απόφασης της Ευρωπαϊκής Επιτροπής[543].

Ο Ν. 2472/1997 εξειδίκευσε και έθεσε το πλαίσιο κατά το οποίο τα κράτη-μέλη καθιστούσαν δυνατή τη διαβίβαση, βάσει της παρ. 1 του άρθρου 25 της Οδηγίας 95/46/ΕΚ. Η διαβίβαση βάσει παρεκκλίσεων, κατόπιν άδειας της Αρχής, εντάχθηκε στην παρ. 2 του άρθρου 9 του Ν. 2472/1997[544]. Επιπλέον, επιβάλλεται να αναφερθεί ότι οι «επαρκείς εγγυήσεις» του άρθρου 26 παρ. 2 της Οδηγίας 95/46/ΕΚ εντάχθηκαν στον κατάλογο των παρεκκλίσεων της παρ. 2 του άρθρου 9 του Ν. 2472/1997[545]. Βέβαια, αξιοσημείωτο είναι ότι οι «επαρκείς εγγυήσεις» προστέθηκαν με την παρ. 3 του άρθρου 24 του Ν. 3471/2006[546] στον κατάλογο των περιπτώσεων της παρ. 2, και πιο συγκεκριμένα αποτέλεσαν την περ. στ της παρ. 2 του άρθρου 9 του Ν. 2472/1997.

Ως προς το εργαλείο διασυνοριακής διαβίβασης των δεσμευτικών εταιρικών κανόνων, χορηγούνταν για αυτό σχετική άδεια από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο πλαίσιο της περ. στ της παρ. 2 του άρθρου 9 του Ν. 2472/1997[547].

---

[543] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 123 κ. επ.

[544] Βλ. Αρμαμέντος, Π., Σωτηρόπουλος, Β. (2005). *Προσωπικά δεδομένα - Ερμηνεία Ν. 2472/1997*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 298 κ. επ.

[545] Για τις αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο πλαίσιο της παραγράφου 2 του άρθρου 9 του Ν. 2472/1997, Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 123 κ. επ.

[546] Βλ. Ν. 3471/2006 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997), (ΦΕΚ Α΄ 133/28-6-2006).

[547] ΑΠΔΠΧ. Αρ. Απόφασης 152/2013

8.4 Η Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Η διασυνοριακή ροή των δεδομένων υγείας[548] μεταξύ των κρατών-μελών της ΕΕ ρυθμίζεται από την Οδηγία 2011/24/ΕΕ[549], η οποία μεταφέρθηκε στην ελληνική έννομη τάξη με το Ν. 4213/2013[550]. Η Οδηγία 2011/24/ΕΕ θεσπίζει τους όρους σύμφωνα με τους οποίους οι ασθενείς δύνανται να λάβουν ιατρική φροντίδα και αποζημίωση από άλλο κράτος-μέλος από αυτό που είναι ασφαλισμένοι[551].

Ειδικότερα, η Οδηγία 2011/24/ΕΕ εισήγαγε, μεταξύ άλλων, στο άρθρο 14 το ηλεκτρονικό δίκτυο eHealth με αντικείμενο την ηλεκτρονική υγεία μεταξύ των κρατών-μελών της ΕΕ και πιο συγκεκριμένα τα δικαιώματα των ασθενών στη διασυνοριακή υγειονομική περίθαλψη[552]. Υπό το πρίσμα της προστασίας των ασθενών ως υποκειμένων των δεδομένων, θα πρέπει, κατά κύριο λόγο, το κράτος θεραπείας να παρέχει ενημέρωση για τα δεδομένα των ασθενών, ενώ το κράτος ασφάλισης να παρέχει ενημέρωση για τα δικαιώματά τους, για την πρόσβαση και άσκηση ένδικων μέσων σε περίπτωση παραβίασης των δικαιωμάτων τους, για τη συνέχιση της θεραπείας στο κράτος ασφάλισης και για την εξ αποστάσεως πρόσβαση στον ιατρικό φάκελο[553]. Στο πλαίσιο του συστήματος που προβλέπει η Οδηγία 2011/24/ΕΕ, είναι απαραίτητο να αναφερθεί ότι δεν περιλαμβάνονται μόνο προσωπικά δεδομένα υγείας με τη στενή έννοια του όρου. Αναμφισβήτητα,

---

[548] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Διασυνοριακή ροή δεδομένων υγείας, Πρακτικά 5ου Συνεδρίου ιατρικής ευθύνης και βιοηθικής – Δεδομένα υγείας και γενετικά δεδομένα, Αθήνα 19 Ιανουαρίου 2018, εκδ. Παπαζήση.

[549] Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 9ης Μαρτίου 2011 περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:02011L0024-20140101

[550] Ν. 4213/2013 (Προσαρμογή της εθνικής νομοθεσίας στις διατάξεις της Οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 9ης Μαρτίου 2011 περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης L 88/45/ 4.4.2011 και άλλες διατάξεις), (ΦΕΚ Α΄/261/3-12-2013).

[551] Ibrahim, M. D., Hocaoglu, M. B., Numan, B., & Daneshvar, S. (2018). Estimating efficiency of Directive 2011/24/EU cross-border healthcare in member states. *Journal of comparative effectiveness research*, *7*(8), 827-834.

[552] European Data Protection Board, European Data Protection Supervisor. (2019). Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI). Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-ehdsi_en

[553] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Διασυνοριακή ροή δεδομένων υγείας, Πρακτικά 5ου Συνεδρίου ιατρικής ευθύνης και βιοηθικής – Δεδομένα υγείας και γενετικά δεδομένα, Αθήνα 19 Ιανουαρίου 2018, εκδ. Παπαζήση.

μπορούν να περιλαμβάνονται και οικονομικά προσωπικά δεδομένα, όπως τα ασφαλιστικά δεδομένα και εν γένει χρηματοοικονομικά δεδομένα[554].

8.5 Ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (GDPR) και ο εφαρμοστικός Ν. 4624/2019

Ο Κανονισμός (ΕΕ) 2016/679[555] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο οποίος αντικατέστησε την Οδηγία 95/46/ΕΚ, αποτελεί τον κεντρικό άξονα του δικαίου των προσωπικών δεδομένων σε ενωσιακό επίπεδο. Ήδη από το 2009 μεθοδεύτηκε η κεντρική αυτή μεταρρύθμιση[556], ως απόρροια των τεχνολογικών αλλαγών οι οποίες είχαν συντελεστεί αφότου θεσπίστηκε η Οδηγία 95/46/ΕΚ[557].

Ειδικότερα, τον Ιανουάριο 2012 παρουσιάστηκε η Πρόταση του Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την προστασία δεδομένων), με αποτέλεσμα τη δημοσίευση, μετά από τροποποιήσεις, στις 4 Μαΐου του 2016 του GDPR, ο οποίος τέθηκε σε εφαρμογή την 25η Μαΐου 2018[558].

Αξίζει να αναφερθεί ότι η μεταρρύθμιση αυτή του πεδίου των προσωπικών δεδομένων στην ΕΕ χρησιμοποίησε ως όχημα της τη δεσμευτική

---

[554] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Διασυνοριακή ροή δεδομένων υγείας, Πρακτικά 5ου Συνεδρίου ιατρικής ευθύνης και βιοηθικής – Δεδομένα υγείας και γενετικά δεδομένα, Αθήνα 19 Ιανουαρίου 2018, εκδ. Παπαζήση.

[555] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[556] Βλ. Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 32.

[557] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα.

[558] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα.

πράξη του Κανονισμού. Αναλυτικότερα, ο Κανονισμός είναι καθολικά δεσμευτικός και έχει άμεση ισχύ για κάθε κράτος-μέλος[559]. Ως εκ τούτου, σκοπός ήταν η άμεση εφαρμογή, χωρίς την ανάγκη υιοθέτησης εθνικού νόμου και η συνεκτικότητα των ρυθμίσεών του[560]. Τα εν λόγω χαρακτηριστικά του GDPR, σημαίνουν αφενός ότι θεσπίζει τους ίδιους κανόνες για την προστασία των προσωπικών δεδομένων στον ΕΟΧ[561] και αφετέρου ότι οι οικονομικές οντότητες των κρατών εκτός ΕΟΧ θα πρέπει να λαμβάνουν υπόψη ένα ενιαίο ευρωπαϊκό νομικό εργαλείο. Ενώ ο GDPR αποτελεί ένα αναλυτικό νομικό κείμενο με 99 άρθρα και 173 αιτιολογικές σκέψεις (η προϊσχύουσα Οδηγία 95/46/ΕΚ είχε 34 άρθρα και 72 αιτιολογικές σκέψεις), εμφανίζει την ευελιξία οδηγίας σε ορισμένα ζητήματα[562] [563]. Ενδεικτικά, δίνεται το δικαίωμα στα κράτη-μέλη να εξειδικεύσουν τον κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου (άρθρο 35 παρ. 4 GDPR) τον καθορισμό της ηλικίας (μεταξύ 13 και 16 ετών) στην οποία προβλέπεται η συγκατάθεση του παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών (άρθρο 8 παρ. 1)[564].

Ως προς το πεδίο της διασυνοριακής ροής των προσωπικών δεδομένων, περιγράφεται καταρχήν στο κεφάλαιο V (άρθρα 44-50) του GDPR υπό τον τίτλο: «Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς

[559] Σαχπεκίδου, Ε. Ρ. (2011). *Ευρωπαϊκό Δίκαιο*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 458 κ. επ.

[560] Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 33.

[561] Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]. Διαθέσιμο στο: https://www.efta.int/sites/default/files/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20English/154-2018.pdf

[562] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα.

[563] Βλ. Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 36.

[564] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ» Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα.

οργανισμούς». Ο Ν. 4624/2019[565] αποτελεί τον ελληνικό εφαρμοστικό νόμο του GDPR. Θα πρέπει να αναφερθεί ότι ο Ν. 4624/2019 δεν περιλαμβάνει διατάξεις που να αντικατοπτρίζουν τα εργαλεία διασυνοριακής διαβίβασης του GDPR, ενώ εμπεριέχει τους μηχανισμούς διασυνοριακής διαβίβασης βάσει της Οδηγίας (ΕΕ) 2016/680 στα άρθρα 75-78 (βλ. υπό 8.6).

8.5.1 Η εξωεδαφικότητα του Κανονισμού

Καταρχάς, το εδαφικό πεδίο εφαρμογής του GDPR προβλέπεται στο άρθρο 3. Το εδαφικό πεδίο εφαρμογής του GDPR εδράζεται, σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων[566], στο κριτήριο της «εγκατάστασης» (άρθρο 3 παρ. 1) και στο κριτήριο της «στόχευσης» (άρθρο 3 παρ. 2). Επιπρόσθετα, η παρ. 3 του άρθρου 3 προβλέπει την περίπτωση εφαρμογής του GDPR, λόγω εφαρμογής του δικαίου κράτους-μέλους βάσει του διεθνούς δικαίου.

Αναλυτικότερα, στην παρ. 1 οριοθετείται η εδαφική εφαρμογή δυνάμει της «εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση». Το γεγονός ότι αναφέρεται η εγκατάσταση του εκτελούντος την επεξεργασία αποτελεί μία καινοτομία του GDPR, αυξάνοντας το πιθανό πεδίο εφαρμογής του[567].

Ομοίως, θα πρέπει να αναφερθεί η αλλαγή που εισάγει το άρθρο 3 παρ. 2 «στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή

[565] Βλ. Ν. 4624/2019 (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις), (ΦΕΚ Α' 137/29-08-2019).

[566] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[567] Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 51 κ. επ.

λαμβάνει χώρα εντός της Ένωσης» [568]. Η επεξήγηση των περιπτώσεων α και β γίνεται στις αιτιολογικές σκέψεις 23 και 24 του GDPR αντίστοιχα[569]. Καθίσταται, λοιπόν, σαφές από την εν λόγω διάταξη ότι ο GDPR δύναται να έχει εξωεδαφική (εκτός ΕΟΧ) εφαρμογή και να απαιτεί την εφαρμογή των διατάξεών του από οντότητες τρίτων κρατών. Η Οδηγία 95/46/ΕΚ στο άρθρο 4 παρ. 1, είχε ως κριτήριο για την εφαρμογή της, την εγκατάσταση του υπεύθυνου της επεξεργασίας[570].

Όσον αφορά την παρ. 3 του άρθρου 3 του GDPR, σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων[571], ο GDPR «εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από πρεσβείες και προξενεία των κρατών μελών της ΕΕ που βρίσκονται εκτός της ΕΕ». Ως εκ τούτου, οι διπλωματικές ή προξενικές αρχές κράτους-μέλους, ως υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία πρέπει να εφαρμόζουν όλες τις διατάξεις του GDPR, μεταξύ άλλων, και τις διατάξεις που αφορούν τη διασυνοριακή διαβίβαση σε τρίτες χώρες[572].

Ως προς τη σχέση των κανόνων της εδαφικής εμβέλειας του GDPR με τους κανόνες της διασυνοριακής διαβίβασης σε τρίτες χώρες, έχει υποστηριχθεί[573] ότι αφενός είναι διαφορετικοί και αφετέρου δύναται να ισχύουν ταυτόχρονα. Η ειδοποιός διαφορά των δύο συνόλων κανόνων είναι ότι οι μηχανισμοί διασυνοριακής διαβίβασης στοχεύουν σε μία ισοδύναμη προστασία των

[568] Βλ. Χρήστου, Β. (2017). Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 227 κ. επ.

[569] Βλ. Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 47 κ. επ.

[570] Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 47 κ. επ.

[571] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[572] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[573] Kuner, C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper*, (20).

προσωπικών δεδομένων με το δίκαιο της ΕΕ, ενώ οι κανόνες εδαφικής εμβέλειας επιβάλλουν την ίδια την εφαρμογή του GDPR[574].

8.5.2 Οι μηχανισμοί της διασυνοριακής ροής δεδομένων σύμφωνα με τον GDPR

Στην παρούσα ενότητα θα αναλυθούν οι μηχανισμοί που προβλέπει ο GDPR για τη διασυνοριακή διαβίβαση προσωπικών δεδομένων, οι οποίοι αναφέρονται στο κεφάλαιο V. Ωστόσο, θα πρέπει να διευκρινιστεί ότι η διασυνοριακή ροή των προσωπικών δεδομένων από τον ΕΟΧ σε τρίτες χώρες δεν είναι ένα στατικό πεδίο. Οι δύο αποφάσεις σταθμοί του ΔΕΕ, οι οποίες καθόρισαν όχι μόνο τις διαβιβάσεις από τον ΕΟΧ στις ΗΠΑ, αλλά και όλες εν γένει τις διαβιβάσεις σε τρίτες χώρες, είναι οι αποφάσεις Schrems I[575] [576] και Schrems II[577] [578]. Επιπρόσθετα, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει εξειδικεύσει πολλά από τα ζητήματα που εγείρουν τα εργαλεία διασυνοριακής διαβίβασης.

Προτού αποσαφηνιστούν τα εργαλεία διαβίβασης, αξίζει να επισημανθεί ότι η καταγραφή της διαβίβασης ή των διαβιβάσεων από τον εξαγωγέα προηγείται του σταδίου διερεύνησης των διαθέσιμων εργαλείων που διαθέτει για την πραγματοποίηση της μεταφοράς των δεδομένων[579]. Στο πλαίσιο της απαραίτητης αυτής χαρτογράφησης περιλαμβάνονται: η εκτίμηση για την πραγματοποίηση ενδεχόμενων διαβιβάσεων, η γνώση της χώρας εισαγωγής και ο

[574] Kuner, C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper*, (20).

[575] C-362/14. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015, Maximillian Schrems κατά Data Protection Commissioner.

[576] Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων). *ΔΙΜΕΕ, 1*, 12-24.

[577] C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

[578] Βλ. Kuner, C. (2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

[579] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

σεβασμός των αρχών επεξεργασίας των προσωπικών δεδομένων. Ειδικότερα για το ζήτημα της αναγνώρισης των διαβιβάσεων σε τρίτες χώρες, θα πρέπει να αναφερθεί ότι ακόμα και η απομακρυσμένη πρόσβαση από τρίτη χώρα συνιστά διαβίβαση, εκτός αν δηλώνεται ότι δεν υπόκεινται σε καμία επεξεργασία στην τρίτη χώρα[580].

8.5.2.1 Απόφαση επάρκειας

Το άρθρο 45 παρ. 1 του GDPR θεσπίζει ως μηχανισμό πρώτης βαθμίδας, ως προς την προστασία των δεδομένων και ως προς τη σειρά επιλογής των διαθέσιμων μηχανισμών, την απόφαση επάρκειας που δίνεται από την Ευρωπαϊκή Επιτροπή, κατόπιν γνώμης του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (αιτιολογική σκέψη 105). Αναλυτικότερα, οι διαβιβάσεις «προς τρίτη χώρα ή διεθνή οργανισμό» πραγματοποιούνται όταν «διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα, από έδαφος ή από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα ή από τον εν λόγω διεθνή οργανισμό» [581].

Ως προς την έννοια του «επαρκούς επιπέδου προστασίας», αξίζει να διευκρινιστεί ότι το «επίπεδο προστασίας» στην τρίτη χώρα πρέπει να είναι «ουσιαστικά ισοδύναμο» με αυτό που εξασφαλίζεται στην ΕΕ, σύμφωνα με την απόφαση Schrems Ι[582]. Πιο συγκεκριμένα, αυτό σημαίνει ότι «τα μέσα που χρησιμοποιεί η χώρα αυτή για να εξασφαλίσει αυτό το επίπεδο προστασίας μπορούν να διαφέρουν από αυτά που εφαρμόζονται εντός της Ένωσης»[583].

Το άρθρο 45 παρ. 2 του GDPR καθορίζει τους παράγοντες τους οποίους αξιολογεί η Ευρωπαϊκή Επιτροπή προκειμένου να εκδώσει μία απόφαση επάρκειας[584]. Η εκτίμηση του επιπέδου προστασίας των δεδομένων της τρίτης

[580] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[581] Ομάδα εργασίας του άρθρου 29. (2018). «Σημεία αναφοράς για την επάρκεια». Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-02/wp254%20rev%200.1_EL.pdf

[582] C-362/14. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015, Maximillian Schrems κατά Data Protection Commissioner.

[583] C-362/14. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015, Maximillian Schrems κατά Data Protection Commissioner.

[584] Ομάδα εργασίας του άρθρου 29. (2018). «Σημεία αναφοράς για την επάρκεια». Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-02/wp254%20rev%200.1_EL.pdf

χώρας ή οργανισμού γίνεται με γνώμονα τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ και τον GDPR, σύμφωνα με την Ομάδα εργασίας του άρθρου 29[585].

Παράλληλα, για την εξέταση του επαρκούς επιπέδου προστασίας λαμβάνονται υπόψη οι «διεθνείς δεσμεύσεις» της τρίτης χώρας ή οργανισμού για την προστασία των δεδομένων (άρθρο 45 παρ. 2 περ. γ). Ιδίως η «προσχώρηση της τρίτης χώρας στη σύμβαση του Συμβουλίου της Ευρώπης της 28ης Ιανουαρίου 1981 για την προστασία των φυσικών προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και στο πρόσθετο πρωτόκολλό της» αποτελεί μία ευνοϊκή παράμετρο, σύμφωνα με την αιτιολογική σκέψη 105. Αξίζει να σημειωθεί ότι από τις 14 χώρες που έχουν λάβει απόφαση επάρκειας[586], οι οποίες περιλαμβάνονται στον παρακάτω πίνακα, οι 5 από αυτές έχουν προσχωρήσει στη Σύμβαση του Συμβουλίου της Ευρώπης της 28ης Ιανουαρίου 1981 και στο πρόσθετο πρωτόκολλό της. Το γεγονός αυτό καταδεικνύει ότι αποτελεί μία ακόμη παράμετρο της εκτιμώμενης επάρκειας, αλλά όχι καταλυτικό παράγοντα στην έκδοση απόφασης.

Στον παρακάτω πίνακα παρατίθενται οι αποφάσεις επάρκειας που έχει εκδώσει η Ευρωπαϊκή Επιτροπή και βρίσκονται σε ισχύ. Η καταγραφή και ταξινόμησή τους έγινε με βάση την ημερομηνία υιοθέτησής τους και με βάση τη νομοθετική ρύθμιση στην οποία εδράζονται («Οι αποφάσεις που εκδόθηκαν βάσει του άρθρου 25 παρ. 6 της Οδηγίας 95/46/ΕΚ παραμένουν σε ισχύ έως ότου τροποποιηθούν, αντικατασταθούν ή καταργηθούν», άρθρο 45 παρ. 9 GDPR).

Η εκάστοτε εξέταση απόφασης επάρκειας από την Ευρωπαϊκή Επιτροπή κινείται εν γένει γύρω από τους βασικούς άξονες, αφενός του περιεχομένου του θεσμικού πλαισίου του τρίτου κράτους και αφετέρου του βαθμού εφαρμογής των νόμων του[587]. Η αξιολόγηση των κανόνων των τρίτων χωρών και η εφαρμογή τους δεν είναι άλλωστε μία στατική διαδικασία αλλά απαιτεί επαγρύπνηση για την αποφυγή μεταβολών (άρθρο 45 παρ. 4) που δύναται να οδηγήσουν και σε ανάκληση αποφάσεων επάρκειας (άρθρο 45 παρ. 5) ή σε ακύρωσή τους από το ΔΕΕ, όπως έγινε για την επάρκεια της προστασίας που παρεχόταν από τις αρχές

[585] Ομάδα εργασίας του άρθρου 29. (2018). «Σημεία αναφοράς για την επάρκεια». Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-02/wp254%20rev%200.1_EL.pdf

[586] Βλ. European Commission. Adequacy decisions. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[587] Ομάδα εργασίας του άρθρου 29. (2018). «Σημεία αναφοράς για την επάρκεια». Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-02/wp254%20rev%200.1_EL.pdf

ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής[588] και της ασπίδας προστασίας της ιδιωτικής ζωής[589], ως προς τις διαβιβάσεις προς τις ΗΠΑ, με τις αποφάσεις Schrems I και Schrems II αντίστοιχα.

Πίνακας 4. Οι αποφάσεις επάρκειας της Ευρωπαϊκής Επιτροπής για τρίτες χώρες[590]

ΑΠΟΦΑΣΕΙΣ ΕΠΑΡΚΕΙΑΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΠΙΤΡΟΠΗΣ	
Αποφάσεις επάρκειας δυνάμει του άρθρου 25 της Οδηγίας 95/46/ΕΚ	**Αποφάσεις επάρκειας δυνάμει του άρθρου 45 του GDPR**
Ελβετία 2000/518/ΕΚ: Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000	**Ιαπωνία** Εκτελεστική απόφαση (ΕΕ) 2019/419 της Επιτροπής, της 23ης Ιανουαρίου 2019
Καναδάς 2002/2/ΕΚ: Απόφαση της Επιτροπής, της 20ής Δεκεμβρίου 2001	**Ηνωμένο Βασίλειο** Εκτελεστική απόφαση της Επιτροπής, της 28ης Ιουνίου 2021
Αργεντινή 2003/490/ΕΚ: Απόφαση της Επιτροπής, της 30ής Ιουνίου 2003	**Νότια Κορέα** Εκτελεστική απόφαση της Επιτροπής, της 17ης Δεκεμβρίου 2021
Γκέρνσεϊ 2003/821/ΕΚ: Απόφαση της Επιτροπής, της 21ης Νοεμβρίου 2003	

[588] 2000/520/ΕΚ: Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32000D0520

[589] Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016D1250

[590] Τα στοιχεία που ταξινομούνται στον πίνακα έχουν αντληθεί από: European Commission. Adequacy decisions. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Νήσος του Μαν 2004/411/ΕΚ: Απόφαση της Επιτροπής, της 28ης Απριλίου 2004	
Τζέρσεϊ 2008/393/ΕΚ: Απόφαση της Επιτροπής, της 8ης Μαΐου 2008	
Φερόες Νήσοι 2010/146/ΕΚ: Απόφαση της Επιτροπής, της 5ης Μαρτίου 2010	
Ανδόρα 2010/625/ΕΕ: Απόφαση της Επιτροπής, της 19ης Οκτωβρίου 2010	
Ισραήλ 2011/61/ΕΕ: Απόφαση της Επιτροπής, της 31ης Ιανουαρίου 2011	
Ουρουγουάη 2012/484/ΕΕ: Εκτελεστική απόφαση της Επιτροπής, της 21ης Αυγούστου 2012	
Νέα Ζηλανδία 2013/65/ΕΕ: Εκτελεστική απόφαση της Επιτροπής, της 19ης Δεκεμβρίου 2012	

8.5.2.2 Κατάλληλες εγγυήσεις

Εάν δεν υπάρχει απόφασης επάρκειας, ο εξαγωγέας των προσωπικών δεδομένων θα πρέπει να στραφεί στα εργαλεία διαβίβασης του άρθρου 46 του GDPR, σύμφωνα με την αιτιολογική σκέψη 108 του Κανονισμού. Οι κατάλληλες εγγυήσεις, μεταξύ του εξαγωγέα και του εισαγωγέα των δεδομένων σε χώρες εκτός ΕΟΧ, λειτουργούν ως μέσα εξασφάλισης επαρκούς επιπέδου προστασίας[591].

[591] Βλ. Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 326 κ. επ.

Τα είδη των εργαλείων διαβίβασης του άρθρου 46 του GDPR, σύμφωνα με την παρ. 2, είναι τα εξής:

α) Νομικά δεσμευτικό και εκτελεστό μέσο μεταξύ δημοσίων αρχών.

β) Δεσμευτικοί εταιρικοί κανόνες (οι οποίοι αναλύονται εκτενώς στην επόμενη ενότητα)

γ) Τυποποιημένες ρήτρες προστασίας δεδομένων θεσπιζόμενες από την Επιτροπή (άρθρο 93 παρ. 2 GDPR)

δ) Τυποποιημένες ρήτρες προστασίας δεδομένων θεσπιζόμενες από την εποπτική αρχή (άρθρο 93 παρ. 2 GDPR)

ε) Εγκεκριμένος κώδικας δεοντολογίας (άρθρο 40 GDPR)

στ) Εγκεκριμένος μηχανισμός πιστοποίησης (άρθρο 42 GDPR).

Παράλληλα, σύμφωνα με την παρ. 3 του άρθρου 46 του GDPR, η αρμόδια εποπτική αρχή μπορεί να παρέχει άδεια, όταν ισχύουν οι ακόλουθες περιπτώσεις[592]:

α) Συμβατικές ρήτρες μεταξύ εισαγωγέα και εξαγωγέα των δεδομένων

β) Διοικητικές ρυθμίσεις μεταξύ δημοσίων αρχών ή φορέων, οι οποίες περιλαμβάνουν εκτελεστά και ουσιαστικά δικαιώματα των υποκειμένων[593].

Ωστόσο, όσον αφορά την εφαρμογή των κατάλληλων εγγυήσεων του άρθρου 46, ο εξαγωγέας των δεδομένων δεν θα πρέπει να επαφίεται μόνο στις διατάξεις του GDPR. Πιο συγκεκριμένα, η απόφαση του ΔΕΕ «Schrems II» έθεσε αυστηρότερα πλαίσια για τις «τυποποιημένες ρήτρες προστασίας δεδομένων»[594], τα οποία δύναται να θεωρηθεί ότι διέπουν όλα τα εργαλεία των «κατάλληλων

[592]Βλ.https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/katallhles_egguhseis

[593] Αναλυτικότερα, η αιτιολογική σκέψη 108 του GDPR αναφέρει ότι: «*…Η άδεια της αρμόδιας εποπτικής αρχής θα πρέπει να αποκτάται εφόσον οι εγγυήσεις προβλέπονται σε νομικά μη δεσμευτικές διοικητικές ρυθμίσεις*.».

[594]Hendrik Mildebrath, European Parliamentary Research Service. (2020). The CJEU judgment in the Schrems II case. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)652073

εγγυήσεων» δυνάμει του άρθρου 46[595]. Η σκέψη 133, της απόφασης της 16ης Ιουλίου 2020, αναφέρει ότι: «ενδέχεται να απαιτείται, ανάλογα με την κατάσταση που επικρατεί στην τάδε ή τη δείνα τρίτη χώρα, η λήψη πρόσθετων μέτρων από τον υπεύθυνο επεξεργασίας προκειμένου να διασφαλίζεται η τήρηση αυτού του επιπέδου προστασίας.»[596]. Θα πρέπει να επισημανθεί ότι το επίπεδο προστασίας που αποτελεί σημείο αναφοράς είναι το επίπεδο που θέτει ο GDPR.

Προκειμένου, λοιπόν, ο εξαγωγέας των προσωπικών δεδομένων να ευθυγραμμίζεται με τις ευρωπαϊκές επιταγές για τις κατάλληλες εγγυήσεις του άρθρου 46, θα πρέπει αυτές να παρέχουν ένα ισοδύναμο επίπεδο προστασίας στην πράξη. Βέβαια, η εξασφάλιση ενός αντίστοιχου επιπέδου με τον ΕΟΧ, προϋποθέτει τη διερεύνηση του επιπέδου προστασίας της τρίτης χώρας εισαγωγής και εν γένει όλου του πλαισίου της εκάστοτε διαβίβασης. Σε περίπτωση που κριθεί ότι δεν εξασφαλίζεται το ισοδύναμο επίπεδο προστασίας με τον ΕΟΧ, θα πρέπει να υιοθετούνται, όπως αναφέρει και η απόφαση Schrems II, «πρόσθετα μέτρα» τα οποία μπορούν να είναι συμβατικού, τεχνικού ή οργανωτικού τύπου[597]. Ως εκ τούτου, η αξιολόγηση πολλών πτυχών του δικαίου των τρίτων χωρών, που μπορούν να επηρεάζουν τη συγκεκριμένη διαβίβαση, επιβάλλει τη μελέτη της νομοθεσίας τους, ενισχύοντας τις υποχρεώσεις του υπεύθυνου της επεξεργασίας. Καθίσταται, λοιπόν, σαφές ότι η υποχρέωση λογοδοσίας έχει προσδώσει, βάσει της απόφασης Schrems II, νέες πτυχές στην εν λόγω αρχή της επεξεργασίας των δεδομένων της παρ. 2 του άρθρου 5 του GDPR.

Πρόσθετη αντίστοιχη εξέλιξη, στο πεδίο των τυποποιημένων ρητρών (άρθρο 46 παρ. 2 περ. γ) ειδικότερα, αποτέλεσε η Εκτελεστική Απόφαση (ΕΕ) 2021/914[598] της Επιτροπής της 4ης Ιουνίου 2021, η οποία δημοσιεύθηκε στην

[595] Kuner, C. (2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

[596] C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

[597] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[598] Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής της 4ης Ιουνίου 2021 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021D0914

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης την 7η Ιουνίου 2021. Η Εκτελεστική Απόφαση (ΕΕ) 2021/914 κατήργησε τις προϋπάρχουσες αποφάσεις 2001/497/ΕΚ και 2010/87/ΕΕ, με τις συμβάσεις που έχουν συναφθεί δυνάμει αυτών να καταργούνται στις 27 Δεκεμβρίου 2022, «υπό την προϋπόθεση ότι οι πράξεις επεξεργασίας που αποτελούν αντικείμενο της σύμβασης παραμένουν αμετάβλητες και ότι η επίκληση των ρητρών αυτών διασφαλίζει ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα υπόκειται σε κατάλληλες εγγυήσεις» (άρθρο 4 Εκτελεστικής Απόφασης (ΕΕ) 2021/914).

Οι κύριες διαφορές των νέων τυποποιημένων ρητρών με τις προηγούμενες έγκεινται στη συμμόρφωση με τις διατάξεις του GDPR (οι καταργηθείσες αποφάσεις ήταν προγενέστερες του GDPR), στην αποτύπωση των νέων απαιτήσεων βάσει της απόφασης Schrems II («Τοπική νομοθεσία και υποχρεώσεις σε περίπτωση πρόσβασης από τις δημόσιες αρχές») και στην προσέγγιση βάσει ενοτήτων, ώστε να παρουσιάζονται σενάρια διαβίβασης[599].

Ως προς τους δημόσιους φορείς εντός ΕΟΧ, οι οποίοι διαβιβάζουν δεδομένα εκτός ΕΟΧ, βάσει κατάλληλων εγγυήσεων, δύνανται να ακολουθήσουν είτε την περίπτωση του νομικά δεσμευτικού και εκτελεστού μέσου (άρθρο 46 παρ. 2 περ. α GDPR) είτε την περίπτωση των διατάξεων προς συμπερίληψη σε διοικητικές ρυθμίσεις (άρθρο 46 παρ. 3 περ. β GDPR)[600]. Επιπρόσθετα, αξίζει να αναφερθεί ότι, στη μεσοπρόθεσμη στρατηγική των οργάνων, γραφείων, φορέων και οργανώσεων της ΕΕ, στο πλαίσιο της συμμόρφωσης με την απόφαση Schrems II, περιλαμβάνεται η διαδικασία εκτίμησης των επιπτώσεων μεταφοράς των δεδομένων (Transfer Impact Assessment)[601].

[599] Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres

[600] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Κατευθυντήριες γραμμές 2/2020 σχετικά με το άρθρο 46 παράγραφος 2 στοιχείο α) και το άρθρο 46 παράγραφος 3 στοιχείο β) του κανονισμού 2016/679 για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και δημόσιων αρχών και φορέων εκτός ΕΟΧ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_el

[601] European Data Protection Supervisor. (2020). Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en

8.5.2.3 Δεσμευτικοί εταιρικοί κανόνες

Οι δεσμευτικοί εταιρικοί κανόνες[602], που αναφέρονται ως εργαλείο διαβίβασης και στο άρθρο 46 GDPR, αναλύονται περαιτέρω στο άρθρο 47 του GDPR. Βέβαια, θα πρέπει να τονιστεί ότι κατέχουν το ίδιο status με τα υπόλοιπα εργαλεία των κατάλληλων εγγυήσεων του άρθρου 46 του GDPR[603], στην κλίμακα των εργαλείων διαβίβασης. Παρατηρείται ότι και το προϊσχύον πλαίσιο της Οδηγίας 95/46/ΕΚ περιελάμβανε τους δεσμευτικούς εταιρικούς κανόνες στην ομπρέλα των κατάλληλων εγγυήσεων[604] [605]. Το ελάχιστο περιεχόμενο των δεσμευτικών εταιρικών κανόνων αναφέρεται στο άρθρο 47 παρ. 2 του GDPR.

Ως προς τη διαδικασία κατάρτισης των δεσμευτικών εταιρικών κανόνων, αυτοί εγκρίνονται από την αρμόδια εποπτική αρχή, σύμφωνα με τον μηχανισμό συνεκτικότητας που ορίζεται στο άρθρο 63 του GDPR, βάσει του οποίου, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων εκδίδει μία μη δεσμευτική γνώμη[606] για το σχέδιο απόφασης το οποίο υποβάλλει η αρμόδια εποπτική αρχή (άρθρο 64 παρ. 1 περ. στ GDPR)[607]. Σε σχέση με την αρμοδιότητα των εποπτικών αρχών για την έγκριση των δεσμευτικών εταιρικών κανόνων, η Ομάδα εργασίας του άρθρου 29[608], έχει προτείνει την αξιολόγηση 5 κριτηρίων: την τοποθεσία της ευρωπαϊκής έδρας του ομίλου (το οποίο θεωρεί ως σημαντικότερο κριτήριο), την

---

[602] «*οι πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις ή δέσμη διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα*». Άρθρο 4 παρ. 20 GDPR.

[603] Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press, p. 765.

[604] Ομάδα εργασίας του άρθρου 29. (2005). «Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995». Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_el.pdf

[605] Article 29 Working Party. (2003). "Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers". Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

[606]Για τις σχετικές γνώμες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, Βλ. https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en?page=2

[607] Article 29 Working Party. (2018). "Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR". Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/623850/en

[608] Article 29 Working Party. (2018). "Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR". Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/623850/en

τοποθεσία στην οποία η οντότητα ασκεί τις υποχρεώσεις της σε σχέση με την προστασία των δεδομένων, την κύρια εγκατάσταση της εταιρείας, ώστε να επιβάλλει τους δεσμευτικούς εταιρικούς κανόνες, την τοποθεσία στην οποία λαμβάνονται οι περισσότερες αποφάσεις όσον αφορά τους σκοπούς και τα μέσα της διαβίβασης και τέλος την τοποθεσία στην οποία πραγματοποιούνται οι περισσότερες διαβιβάσεις εκτός ΕΟΧ.

Όσον αφορά το πεδίο εφαρμογής των δεσμευτικών εταιρικών κανόνων, οι διαβιβάσεις δεδομένων δύναται να απευθύνονται σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα[609]. Οι δεσμευτικοί εταιρικοί κανόνες είναι καταρχήν νομικά δεσμευτικοί και θα πρέπει να εφαρμόζονται από κάθε εμπλεκόμενο μέρος του ομίλου[610]. Επιπρόσθετα, θα πρέπει να αναφερθεί ότι οι δεσμευτικοί εταιρικοί κανόνες δεν μπορούν να χρησιμοποιηθούν από έναν υπεύθυνο επεξεργασίας δεδομένων ή εκτελούντα για τις μεταφορές δεδομένων που αποστέλλονται σε μέρη εκτός του εταιρικού πλέγματος, όπως οι πελάτες και οι προμηθευτές[611].

Αξίζει να επισημανθεί ότι τα κύρια σημεία που έθεσε η απόφαση Schrems ΙΙ[612] αφορούν και τους εταιρικούς δεσμευτικούς κανόνες ως κατηγορία των κατάλληλων εγγυήσεων της παρ. 2 του άρθρου 46 του GDPR[613]. Αναλυτικότερα, ο εξαγωγέας και ο εισαγωγέας των προσωπικών δεδομένων θα πρέπει να αξιολογούν, και στην περίπτωση των εταιρικών δεσμευτικών κανόνων, το επίπεδο προστασίας των δεδομένων στην τρίτη χώρα, και να εφαρμόζουν συμπληρωματικά μέτρα εάν κρίνεται απαραίτητο[614].

---

[609]Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/bcr

[610]Βλ. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[611]Leung, R. (2018). Cross-border data transfers under the GDPR: a perspective from non-European e-commerce businesses.

[612]Βλ. C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

[613]Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[614]Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. Update of Selected Articles (May 4, 2021).

8.5.2.4 Παρεκκλίσεις για ειδικές καταστάσεις της παρ. 1 εδ. 1 του άρθρου 49

Καταρχάς, οι εξαγωγείς των δεδομένων, όπως υποδηλώνει και ο ίδιος ο όρος που επιλέχθηκε για τη διάταξη, επιβάλλεται να καταφεύγουν σε αυτές τις «εξαιρέσεις», εφόσον προηγουμένως αποκλείσουν τη δυνατότητα αξιοποίησης των εργαλείων των άρθρων 45 και 46 του GDPR κατά σειρά[615].

Πιο συγκεκριμένα, όπως έχει υποστηριχθεί[616], ο δικαιολογητικός λόγος των παρεκκλίσεων (εφόσον έχουν αποκλειστεί τα εργαλεία των άρθρων 45 και 46 του GDPR) είναι η πραγματοποίηση μίας διαβίβασης όταν υπάρχει υπέρτερο κοινωνικό συμφέρον, είτε λόγω ύπαρξης ελάχιστων κινδύνων είτε λόγω ύπαρξης υπέρτερων δικαιωμάτων και συμφερόντων. Ως εκ τούτου, διαφαίνεται πως, ως «συγκεκριμένες περιπτώσεις», οι παρεκκλίσεις θα πρέπει να μην αποτελούν ένα πάγιο μέτρο[617] [618].

Οι περιπτώσεις των παρεκκλίσεων για ειδικές καταστάσεις της παρ. 1 εδ. 1 του άρθρου 49, είναι οι εξής:

α) Το υποκείμενο έχει ενημερωθεί για τους πιθανούς κινδύνους μιας τέτοιας διαβίβασης και έχει ρητώς συγκατατεθεί στη συγκεκριμένη διαβίβαση.

β) Η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υποκειμένου και του υπευθύνου επεξεργασίας ή την εφαρμογή προσυμβατικών μέτρων κατόπιν αιτήματος του υποκειμένου.

γ) Η διαβίβαση είναι απαραίτητη για τη σύναψη ή εκτέλεση σύμβασης συναφθείσας προς όφελος του υποκειμένου μεταξύ του υπευθύνου επεξεργασίας και άλλου φυσικού ή νομικού προσώπου.

---

[615] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[616] Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press, p. 843.

[617] Article 29 Working Party. (1998). "Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive". Διαθέσιμο στο: https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/1998/wp12_en.pdf

[618] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

δ) Η διαβίβαση είναι απαραίτητη για σπουδαίους λόγους δημοσίου συμφέροντος που αναγνωρίζονται είτε στη νομοθεσία της ΕΕ είτε στη νομοθεσία κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας.

ε) Η διαβίβαση είναι απαραίτητη για τη θεμελίωση, άσκηση ή υπεράσπιση νομικών αξιώσεων.

στ) Η διαβίβαση είναι απαραίτητη προκειμένου να προστατευθούν τα ζωτικά συμφέροντα του υποκειμένου ή άλλων προσώπων, όταν το υποκείμενο είναι φυσικά ή νομικά ανίκανο να παρέχει συγκατάθεση.

ζ) Η διαβίβαση πραγματοποιείται από μητρώο ανοιχτό στο κοινό ή έπειτα από αίτημα σε κάθε πρόσωπο που μπορεί να θεμελιώσει έννομο συμφέρον στην πρόσβαση σε αυτό[619].

Θα πρέπει να σημειωθεί ότι, σύμφωνα με την παρ. 3 του άρθρου 49 GDPR, οι τρεις πρώτες περιπτώσεις των ανωτέρω παρεκκλίσεων «δεν εφαρμόζονται σε δραστηριότητες που εκτελούνται από δημόσιες αρχές κατά την άσκηση των δημόσιων εξουσιών τους».

Παράλληλα, θα πρέπει να αναφερθεί ότι η αιτιολογική σκέψη 111 του GDPR θέτει μία επιπλέον προϋπόθεση στις παρεκκλίσεις των περιπτώσεων β, γ και ε, οι οποίες αφορούν «σύμβαση» ή «νομική αξίωση» αντίστοιχα[620]. Περαιτέρω, σύμφωνα με το εδ. 1 της αιτιολογικής σκέψης 111: «Θα πρέπει να προβλεφθεί η δυνατότητα διαβιβάσεων σε ορισμένες περιπτώσεις, όταν το υποκείμενο των δεδομένων παρέσχε τη ρητή συγκατάθεσή του, εφόσον η διαβίβαση είναι περιστασιακή και αναγκαία σε σχέση με σύμβαση ή με νομική αξίωση, είτε σε δικαστική διαδικασία είτε σε διοικητική ή τυχόν εξωδικαστική διαδικασία, μεταξύ άλλων σε διαδικασίες ενώπιον ρυθμιστικών φορέων…».

Ειδικότερα, όσον αφορά την περ. δ της παρ. 1 του άρθρου 49, η οποία αναφέρεται στους «σπουδαίους λόγους δημοσίου συμφέροντος», θα πρέπει να επισημανθεί ότι, σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας

[619] Βλ. https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/parekliseis

[620] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

Δεδομένων[621], δύναται να αποτελέσει εργαλείο που χρησιμοποιείται και από ιδιωτικές οικονομικές οντότητες. Ως εκ τούτου, το εν λόγω εργαλείο μπορεί να αποτελέσει το μέσο των κομβικών περιπτώσεων της διασυνοριακής ροής οικονομικών δεδομένων, της αιτιολογικής σκέψης 112 του GDPR και πιο συγκεκριμένα των «διεθνών ανταλλαγών δεδομένων μεταξύ αρχών ανταγωνισμού, φορολογικών ή τελωνειακών αρχών, μεταξύ αρχών χρηματοοικονομικής εποπτείας, μεταξύ υπηρεσιών αρμόδιων για θέματα κοινωνικής ασφάλισης».

8.5.2.5 Η περιορισμένη παρέκκλιση της παρ. 1 εδ. 2 του άρθρου 49

Το εδάφιο β της παρ. 1 του άρθρου 49 του GDPR, περιλαμβάνει μία ακόμα παρέκκλιση, στενότερη, η οποία, ωστόσο, δεν έχει αριθμηθεί στο πλαίσιο της διάταξης[622].

Η παρέκκλιση του εδ. 2 αποτελεί το τελευταίο εργαλείο στο οποίο θα πρέπει ο εξαγωγέας των δεδομένων να στρέφεται, αφού, σύμφωνα με την εν λόγω διάταξη, θα πρέπει προηγουμένως να έχει αποκλείσει τη δυνατότητα χρήσης των εργαλείων της απόφασης επάρκειας, των κατάλληλων εγγυήσεων καθώς και των υπόλοιπων παρεκκλίσεων του εδ. 1 της παρ. 1 του άρθρου 49. Σύμφωνα με την αιτιολογική σκέψη 113: «…Οι διαβιβάσεις αυτές θα πρέπει να είναι δυνατές μόνο στις περιπτώσεις στις οποίες δεν συντρέχει κανένας από τους άλλους λόγους μεταβίβασης…». Κατά συνέπεια, λαμβάνοντας υπόψη την αρχή της λογοδοσίας του υπεύθυνου της επεξεργασίας, οφείλει ο εξαγωγέας των δεδομένων να αποδείξει την προσφυγή σε αυτό το εργαλείο τελευταίας επιλογής[623].

Οι προϋποθέσεις που θέτει η παρέκκλιση του εδ. 2, θα πρέπει να ισχύουν σωρευτικά και είναι οι εξής: «…εάν η διαβίβαση δεν είναι επαναλαμβανόμενη, αφορά μόνο περιορισμένο αριθμό υποκειμένων των δεδομένων, είναι απαραίτητη για τους σκοπούς επιτακτικών έννομων συμφερόντων που επιδιώκει ο υπεύθυνος

[621] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[622] Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press, p. 847.

[623] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

επεξεργασίας των οποίων δεν υπερισχύουν τα συμφέροντα ή τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων και ο υπεύθυνος επεξεργασίας έχει εκτιμήσει όλες τις περιστάσεις που σχετίζονται με τη διαβίβαση των δεδομένων και έχει παράσχει, βάσει της εν λόγω εκτίμησης, τις δέουσες εγγυήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα.»

Η υποχρέωση που θέτει η αιτιολογική σκέψη 113 (περί απόδειξης από τον εξαγωγέα ως προς την αναγκαιότητα χρήσης αυτού του ειδικού εργαλείου), αλλά και οι πολλές προϋποθέσεις που θέτει το ίδιο το εδ. 2 της παρ. 1 του άρθρου 49, δύνανται να αποτελέσουν εμπόδια για τον εξαγωγέα, επιδιώκοντας την περιορισμένη χρήση του εν λόγω εργαλείου στις διασυνοριακές διαβιβάσεις προσωπικών δεδομένων σε τρίτα κράτη.

8.5.2.6 Μεταφορά δεδομένων βάσει διεθνούς συμφωνίας, σε εφαρμογή απόφασης δικαστηρίου και διοικητικής αρχής τρίτης χώρας

Το άρθρο 48 προβλέπει ότι οι αποφάσεις διοικητικών αρχών και δικαστηρίων τρίτης χώρας δεν αποτελούν νόμιμους λόγους για τη διαβίβαση δεδομένων σε τρίτες χώρες, εκτός αν επιτρέπεται από διεθνή συμφωνία[624]. Είναι αναγκαίο να αναφερθεί ότι η διάταξη αυτή λειτουργεί περισσότερο ως περιορισμός διασυνοριακής διαβίβασης[625], παρά ως εργαλείο διαβίβασης όπως τα υπόλοιπα άρθρα του κεφαλαίου V του GDPR, όπως υποδεικνύει και ο τίτλος του: «*Διαβιβάσεις ή κοινοποιήσεις που δεν επιτρέπονται από το δίκαιο της Ένωσης*».

Παράλληλα, θα πρέπει να τονιστεί ότι, σύμφωνα με το άρθρο 48, όταν υφίσταται απόφαση δικαστηρίου ή διοικητικής αρχής τρίτης χώρας, μπορεί να αποτελέσει βάση της διαβίβασης μόνο όταν υφίσταται διεθνής συμφωνία, με την επιφύλαξη όμως των εργαλείων διαβίβασης του κεφαλαίου V. Αυτό συνεπάγεται, σε συνδυασμό με την Κοινή Απάντηση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων και του Ευρωπαίου Επόπτη Προστασίας Δεδομένων στον νόμο US

[624] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

[625] Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press, p. 830.

Cloud Act[626], ότι μία τέτοια διαβίβαση στο πλαίσιο του άρθρου 48 θα πρέπει να βασίζεται στα άρθρα 6 και 49 του GDPR[627].

8.5.3 Η Αρμοδιότητα των εποπτικών αρχών και επιβολή διοικητικών προστίμων

Για τις διασυνοριακές πράξεις επεξεργασίας (όπως ορίζονται στο άρθρο 4 περ. 23 GDPR), επικεφαλής εποπτική αρχή είναι η εποπτική αρχή της χώρας στην οποία βρίσκεται η κύρια ή μόνη εγκατάσταση του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (άρθρο 56 παρ. 1 GDPR). Επομένως, η εξεύρεση της επικεφαλής εποπτικής αρχής απαιτείται όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει εγκατάσταση σε περισσότερα από ένα κράτη-μέλη ή έχει μία εγκατάσταση αλλά «επηρεάζει ουσιωδώς» υποκείμενα δεδομένων άλλου κράτους-μέλους [628] [629].

Το ΔΕΕ στην πρόσφατη απόφαση[630] της υπόθεσης C-645/19 υπογράμμισε ότι στην περίπτωση διασυνοριακής επεξεργασίας δεδομένων, και ειδικότερα στο πλαίσιο του άρθρου 58 παρ. 5 του GDPR, «εποπτική αρχή κράτους μέλους διαφορετική από την επικεφαλής εποπτική αρχή μπορεί να κινεί ένδικες διαδικασίες, κατά την έννοια της διατάξεως αυτής, χωρίς να απαιτείται ο υπεύθυνος επεξεργασίας ή ο εκτελών τη διασυνοριακή επεξεργασία δεδομένων προσωπικού χαρακτήρα, κατά του οποίου στρέφεται η ένδικη διαδικασία, να διαθέτει κύρια εγκατάσταση ή άλλη εγκατάσταση στο έδαφος του κράτους μέλους αυτού».

Τα καθήκοντα των αρμοδίων εποπτικών αρχών, που θεσπίζονται στο άρθρο 57, περιλαμβάνουν στις περ. ιη και ιθ την παροχή άδειας των συμβατικών ρητρών και διατάξεων του άρθρου 46 παρ. 3 και την έγκριση των δεσμευτικών

[626] EDPB, EDPS. (2019). "Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection". Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en

[627] Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press, p. 831.

[628] Ομάδα εργασίας του άρθρου 29. (2016). «Κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία». Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/itemType/1360

[629] Βλ. https://www.dpa.gr/el/foreis/prosdiorismos_epikefalis_arxis

[630] C-645/19. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 5ης Ιουνίου 2021, Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA κατά Gegevensbeschermingsautoriteit.

εταιρικών κανόνων του άρθρου 47. Στην περίπτωση διασυνοριακής πράξης επεξεργασίας, οι ανωτέρω εξουσίες ανήκουν στην επικεφαλής εποπτική αρχή[631].

Σε περίπτωση παραβίασης των διατάξεων για τα εργαλεία διαβίβασης (άρθρα 44-49 GDPR), το διοικητικό πρόστιμο που επιβάλλεται από την αρμόδια εποπτική αρχή μπορεί να είναι «έως 20.000.000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο», σύμφωνα με το άρθρο 83 παρ. 5 περ. γ.

8.5.4 Συγκριτική αποτίμηση της ρύθμισης της διασυνοριακής ροής δεδομένων στην Οδηγία 95/46/ΕΚ και στον Κανονισμό (ΕΕ) 2016/679

Στο πεδίο των διασυνοριακών ροών των προσωπικών δεδομένων, ο GDPR διατηρεί τους τρείς κύριους μηχανισμούς διασυνοριακών ροών (απόφαση επάρκειας, κατάλληλες εγγυήσεις, παρεκκλίσεις)[632], αναλύοντας όμως περισσότερο το πλαίσιο εφαρμογής τους. Στην παρούσα ενότητα θα πραγματοποιηθεί μία σύγκριση σε σχέση με τις κύριες και με αντίκτυπο αλλαγές που έχει επιφέρει ο GDPR σε σχέση με την Οδηγία 95/46/ΕΚ, με σημείο αναφοράς το κάθε εργαλείο διασυνοριακής διαβίβασης των προσωπικών δεδομένων.

Πιο συγκεκριμένα, σε σχέση με την επάρκεια της τρίτης χώρας ως βάση διασυνοριακής διαβίβασης, το «ικανοποιητικό επίπεδο της τρίτης χώρας» (άρθρο 25 παρ. της Οδηγίας 95/46/ΕΚ) δεν κρίνεται πλέον από το κράτος-μέλος (αρμόδια εποπτική αρχή)[633]. Σύμφωνα με τον GDPR (άρθρο 45), μόνο η Ευρωπαϊκή Επιτροπή αποφαίνεται για διαβιβάσεις βάσει απόφασης επάρκειας του επιπέδου προστασίας των δεδομένων των τρίτων χωρών, αφαιρώντας την καίρια αυτή αρμοδιότητα από τις εθνικές αρχές.

Όσον αφορά τις «επαρκείς εγγυήσεις» της Οδηγίας 95/46/ΕΚ (άρθρο 26 παρ. 2), μετονομάστηκαν σε «κατάλληλες εγγυήσεις» στον GDPR (άρθρο 46

---

[631] Βλ. Κόμνιος, Κ. (2020). *Γενικός κανονισμός για την προστασία δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 17 κ. επ.

[632] Kuner, C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper*, (20).

[633] Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2019). Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων. *ΔΙΜΕΕ, 4*, 504-520.

GDPR) [634] και έλαβαν ξεχωριστό άρθρο στον Κανονισμό, καταδεικνύοντας τη σημασία αυτού του μηχανισμού. Ειδικότερα ως προς τους δεσμευτικούς εταιρικούς κανόνες, όπως αναφέρει η ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[635], ο GDPR αποτύπωσε συμπεράσματα της Ομάδας εργασίας του άρθρου 29, διευρύνοντας την εφαρμογή τους όχι μόνο σε ομίλους επιχειρήσεων (άρθρο 4 περ. 20 GDPR), αλλά και σε χαλαρότερες μορφές συνεργασίας, πέραν των ομίλων επιχειρήσεων.[636]

Στο πεδίο του εργαλείου διαβίβασης των παρεκκλίσεων, ο GDPR δεν απαιτεί άδεια της αρμόδιας εποπτικής αρχής στο άρθρο 49, αφαιρώντας αυτήν την εξουσία από τις εθνικές αρχές[637]. Αναλυτικότερα, η παρ. 1 του άρθρου 26 της Οδηγίας 95/46/ΕΚ αναφέρονταν σε άδεια των κρατών-μελών για τις διαβιβάσεις βάσει παρεκκλίσεων, που στον ελληνικό Ν. 2472/1997 εξειδικεύτηκε σε άδεια της εποπτικής αρχής (άρθρο 9 παρ. 2). Συνεπώς, καθίσταται προφανής η πρόθεση, μέσω του GDPR, αποδέσμευσης των εθνικών εποπτικών αρχών από την έκδοση σχετικών αδειών για τις διαβιβάσεις βάσει παρεκκλίσεων με παράλληλη ενίσχυση της υποχρέωσης λογοδοσίας του εξαγωγέα των δεδομένων.

Ειδικότερα, ως προς την περιορισμένη παρέκκλιση της παρ. 1 εδ. 2 του άρθρου 49 του GDPR, θα πρέπει να αναφερθεί ότι αυτός ο μηχανισμός δεν περιλαμβανόταν προηγουμένως στην Οδηγία 95/46/ΕΚ[638]. Εισάγεται, υπό τις στενές προϋποθέσεις της διάταξης, αυτός ο μηχανισμός διασυνοριακής διαβίβασης, ο οποίος όμως έχοντας πολύ συγκεκριμένες περιπτώσεις εφαρμογής, δεν επιδιώκει ενδεχομένως να αυξήσει το πεδίο εφαρμογής των παρεκκλίσεων, αλλά να προστατεύσει περαιτέρω τα υποκείμενα των δεδομένων με την υποχρέωση ενημέρωσης αυτών αλλά και της αρμόδιας εποπτικής αρχής.

Οι διαβιβάσεις δεδομένων σε τρίτες χώρες, σε γενικές γραμμές, θα μπορούσε να υποστηριχθεί ότι αντιμετωπίστηκαν από τον GDPR με πιο συστηματικό τρόπο από ό,τι στην Οδηγία 95/46/ΕΚ, αντικατοπτρίζοντας τη

[634]Kuner, C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper*, (20).

[635]Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/bcr

[636]Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/bcr

[637]Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2019). Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων. *ΔΙΜΕΕ, 4*, 504-520.

[638]Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

σημασία των διασυνοριακών ροών και λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις που μεσολάβησαν στις δύο δεκαετίες που χωρίζουν τα δύο αυτά σημεία αναφοράς της προστασίας των προσωπικών δεδομένων στην ΕΕ.

8.6 Η Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και ο εφαρμοστικός Ν. 4624/2019

Η Οδηγία (ΕΕ) 2016/680[639] θεσπίζει το ειδικό πλαίσιο της επεξεργασίας των προσωπικών δεδομένων από τις αρμόδιες αρχές «για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους». Ο Ν. 4624/2019[640] μετέφερε στην Ελλάδα την Οδηγία (ΕΕ) 2016/680[641], όπως και τα μέτρα εφαρμογής του GDPR. Αναλυτικότερα, στα άρθρα 75-78 του Ν. 4624/2019 περιλαμβάνονται οι μηχανισμοί διασυνοριακής διαβίβασης βάσει της Οδηγίας (ΕΕ) 2016/680.

Η Οδηγία (ΕΕ) 2016/680 θεσπίζει τους μηχανισμούς διαβίβασης των προσωπικών δεδομένων προς τρίτη χώρα ή διεθνή οργανισμό στα άρθρα 35-39[642].

[639]Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016L0680

[640]Βλ. Ν. 4624/2019 (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις), (ΦΕΚ Α' 137/29-08-2019).

[641]Βλ. Παναγοπούλου-Κουτνατζή, Φ. (2019). Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων. *ΔΙΜΕΕ, 4*, 504-520.

[642]Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2021). «Συστάσεις 1/2021 σχετικά με τα σημεία αναφοράς για την επάρκεια βάσει της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

Η διαβίβαση δεδομένων επιτρέπεται, σύμφωνα με το άρθρο 35 της Οδηγίας (ΕΕ) 2016/680, στις ακόλουθες περιπτώσεις[643]:

- Η διαβίβαση είναι αναγκαία για τους σκοπούς που ορίζει η Οδηγία (ΕΕ) 2016/680. (περ. α και β του άρθρου 35)
- Το κράτος-μέλος στο οποίο διαβιβάζονται ή καθίστανται διαθέσιμα τα προσωπικά δεδομένα έχει παράσχει την έγκρισή του για τη διαβίβαση σύμφωνα με το εθνικό του δίκαιο. (περ. γ του άρθρου 35)
- Η Ευρωπαϊκή Επιτροπή έχει εκδώσει απόφαση επάρκειας (άρθρο 36), έχουν θεσπιστεί κατάλληλες εγγυήσεις (άρθρο 37) ή ισχύει η παρέκκλιση για τις διαβιβάσεις σε ειδικές περιπτώσεις (άρθρο 38). (περ. δ του άρθρου 35)
- «Η περαιτέρω διαβίβαση προσωπικών δεδομένων προς άλλη τρίτη χώρα ή διεθνή οργανισμό προϋποθέτει την προηγούμενη έγκριση της αρμόδιας αρχής προέλευσης, η οποία λαμβάνει υπόψη, μεταξύ άλλων, τη σοβαρότητα του αδικήματος και το επίπεδο προστασίας των δεδομένων στη χώρα προορισμού της δεύτερης διεθνούς διαβίβασης»[644]. (περ. ε του άρθρου 35)

Η Οδηγία (ΕΕ) 2016/680, ακολουθώντας το μοντέλο της διασυνοριακής ροής των προσωπικών δεδομένων σε τρίτες χώρες του GDPR αλλά και της προϊσχύουσας Οδηγίας 95/46/ΕΚ, προβλέπει την απόφαση επάρκειας, τις κατάλληλες εγγυήσεις και τις παρεκκλίσεις. Η επιλογή των εργαλείων από τον εξαγωγέα γίνεται και σε αυτό το νομοθετικό εργαλείο σύμφωνα με τη σειρά αναφοράς[645]. Ειδικότερα για την απόφαση επάρκειας, θα πρέπει να αναφερθεί ότι αποφάσεις επάρκειας, δυνάμει του GDPR και της Οδηγίας 95/46/ΕΚ, δεν καλύπτουν τις διαβιβάσεις των δεδομένων στο πλαίσιο της Οδηγίας (ΕΕ) 2016/680), με εξαίρεση την απόφαση επάρκειας για το Ηνωμένο Βασίλειο[646].

---

[643] Βλ. Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 364 κ. επ.

[644] Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 364 κ. επ.

[645] Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 364 κ. επ.

[646] European Commission. Adequacy decisions. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

8.7 Η Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Η Οδηγία (ΕΕ) 2016/681[647] θεσπίζει το πλαίσιο της διαβίβασης των δεδομένων PNR (passenger name records, καταστάσεις ονομάτων επιβατών), (βλ. και υπό 9.2.1) των διεθνών πτήσεων προς και από την ΕΕ, καθώς και των πτήσεων εντός της ΕΕ, με σκοπό την πρόληψη, την ανίχνευση, τη διερεύνηση ή τη δίωξη τρομοκρατικών και σοβαρών εγκλημάτων[648]. Η Οδηγία (ΕΕ) 2016/681 μεταφέρθηκε στο εθνικό δίκαιο της Ελλάδας με τον Ν. 4579/2018[649], ο οποίος αφορά τη διαβίβαση των δεδομένων από τους αερομεταφορείς πτήσεων εντός ή εκτός της ΕΕ, οι οποίες προσγειώνονται ή απογειώνονται σε/από ελληνικό έδαφος, καθώς και στην επεξεργασία, στη συλλογή, στη χρήση και διατήρηση, αλλά και στην ανταλλαγή των δεδομένων αυτών με τα υπόλοιπα κράτη-μέλη (άρθρο 2 Ν. 4579/2018)[650].

Η Οδηγία (ΕΕ) 2016/681 θεσπίζει τις προϋποθέσεις διαβίβασης των δεδομένων PNR σε τρίτες χώρες στο άρθρο 11. Η διαβίβαση των δεδομένων PNR στις αρμόδιες αρχές τρίτων χωρών γίνεται σύμφωνα με όρους που συνάδουν με την Οδηγία, λαμβάνοντας υπόψη και τη «σκοπούμενη χρήση» των δεδομένων από τους παραλήπτες σύμφωνα με την παρ. 3 του άρθρου 11. Επιπλέον, θα πρέπει να επισημανθεί η υποχρέωση, που θεσπίζει η Οδηγία στο άρθρο 11 παρ. 4, και αφορά την ενημέρωση του υπεύθυνου προστασίας δεδομένων της μονάδας στοιχείων επιβατών του εκάστοτε κράτους-μέλους, κάθε φορά που το κράτος μέλος διαβιβάζει τα εν λόγω δεδομένα σε τρίτες χώρες. Θα πρέπει ακόμη να σημειωθεί ότι στο πλαίσιο της Οδηγίας (ΕΕ) 2016/681 δεν επιτρέπεται «η συλλογή και χρήση ευαίσθητων δεδομένων» και ως εκ τούτου η διαβίβασή τους (αιτιολογική σκέψη 37).

---

[647] Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L0681

[648] Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 335, 372.

[649] Ν. 4579/2018 (Υποχρεώσεις αερομεταφορέων σχετικά με τα αρχεία επιβατών προσαρμογή της νομοθεσίας στην Οδηγία (ΕΕ) 2016/681 και άλλες διατάξεις), (ΦΕΚ Α' 201/03-12-2018).

[650] Βλ. Ιγγλεζάκης, Ι. (2021). *Δίκαιο Πληροφορικής*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 362 κ. επ.

Όσον αφορά τη διατήρηση των διαβιβαζόμενων δεδομένων σε βάση δεδομένων, θα πρέπει να αναφερθεί ότι η Οδηγία θέτει το χρονικό όριο των πέντε ετών (άρθρο 12 παρ. 1). Παράλληλα, τα διαβιβαζόμενα δεδομένα θα πρέπει να ανωνυμοποιούνται έξι μήνες μετά τη διαβίβασή τους.

8.8 Ο Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Ο Κανονισμός (ΕΕ) 2018/1725[651], ο οποίος αφορά την προστασία των προσωπικών δεδομένων από τα θεσμικά, λοιπά όργανα και οργανισμούς της ΕΕ, περιλαμβάνει στο κεφάλαιο V τους μηχανισμούς διασυνοριακών διαβιβάσεων των προσωπικών δεδομένων, οι οποίοι εμφανίζουν αντιστοιχία με τον GDPR[652].

Καταρχάς, θα πρέπει να αναφερθεί ότι ο πυρήνας των εργαλείων διασυνοριακής διαβίβασης του Κανονισμού (ΕΕ) 2018/1725 και του GDPR είναι ίδιος[653]. Πιο συγκεκριμένα, αν τα θεσμικά όργανα και οι οργανισμοί της ΕΕ δεν μπορούν να χρησιμοποιήσουν την απόφαση επάρκειας ως εργαλείο διαβίβασης (άρθρο 47), τότε στρέφονται στις κατάλληλες εγγυήσεις (άρθρο 48). Εάν δεν παρέχονται κατάλληλες εγγυήσεις, τα θεσμικά όργανα και οι οργανισμοί της ΕΕ θα πρέπει να αναζητήσουν παρεκκλίσεις, αξιολογώντας αν αυτές εμπίπτουν στην περίπτωση της συγκεκριμένης διαβίβασης[654] [655]. Επιπρόσθετα, θα πρέπει να σημειωθεί ότι η απόφαση επάρκειας, ως εργαλείο διαβίβασης στο πλαίσιο του εν

[651] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018R1725

[652] Tracol, X. (2021). Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations. In *ERA Forum* (pp. 1-16). Springer Berlin Heidelberg.

[653] Βλ. European Data Protection Supervisor. (2020). Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en

[654] European Data Protection Supervisor. (2020). Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en

[655] Tracol, X. (2021). Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations. In *ERA Forum* (pp. 1-16). Springer Berlin Heidelberg.

λόγω Κανονισμού, μπορεί να εδράζεται τόσο στον GDPR όσο και στην Οδηγία (ΕΕ) 2016/680 (άρθρο 47 παρ. 1 Κανονισμού (ΕΕ) 2018/1725).

Σύμφωνα με τον δημοσιευθέντα στρατηγικό σχεδιασμό[656] των οργάνων, γραφείων, φορέων και οργανώσεων της ΕΕ, στο πλαίσιο της συμμόρφωσης με την απόφαση Schrems II, ως βραχυπρόθεσμη ενέργεια προτάθηκε η διαδικασία της χαρτογράφησης των συμβάσεων, των διαδικασιών προμηθειών και άλλων ειδών συνεργασίας οι οποίες απαιτούν διαβίβαση δεδομένων σε τρίτες χώρες. Ως μεσοπρόθεσμη ενέργεια προτάθηκε η διαδικασία εκτίμησης των επιπτώσεων μεταφοράς των δεδομένων (Transfer Impact Assessment).

[656] European Data Protection Supervisor. (2020). Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en

ΚΕΦΑΛΑΙΟ 9. Η ΝΟΜΙΚΗ ΡΥΘΜΙΣΗ ΤΗΣ ΔΙΑΣΥΝΟΡΙΑΚΗΣ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΗΝ ΕΕ ΣΤΙΣ ΗΠΑ

9.1 Εισαγωγικές παρατηρήσεις

Στο παρόν κεφάλαιο, αναλύεται το πλαίσιο των διασυνοριακών ροών των προσωπικών δεδομένων, ειδικότερα υπό τη θέση της ΕΕ ως εξαγωγέα των δεδομένων και των ΗΠΑ ως εισαγωγέα αντίστοιχα. Αναλυτικότερα, αποσαφηνίζονται οι κύριες συμφωνίες σε αυτό το πεδίο και η διαχρονική πορεία της νομικής ρύθμισης της διατλαντικής[657] μεταφοράς των προσωπικών δεδομένων, λαμβάνοντας υπόψη τους κυριότερους σταθμούς αυτού του πεδίου. Η διερεύνηση της διατλαντικής μεταφοράς των προσωπικών δεδομένων είναι ιδιαίτερα σημαντική, αφενός λόγω του μεγάλου όγκου οικονομικών δεδομένων που περικλείει στο πλαίσιο των επιχειρηματικών σχέσεων που αναπτύσσονται μεταξύ των δύο πλευρών του ατλαντικού, και αφετέρου λόγω της επιρροής αυτής της σχέσης σε όλες τις διασυνοριακές ροές των προσωπικών δεδομένων από την ΕΕ, ιδιαίτερα μέσω της νομολογίας του ΔΕΕ.

9.2 Συμφωνίες για τη διασυνοριακή ροή δεδομένων της ΕΕ με τις ΗΠΑ

Μεταξύ των κυβερνήσεων των δύο χωρών του ατλαντικού, εκτός του γενικού πλαισίου μεταφοράς προσωπικών δεδομένων, υφίστανται και οι διεθνείς συμφωνίες οι οποίες διασφαλίζουν την προστασία των προσωπικών δεδομένων για σκοπούς επιβολής του νόμου[658]. Τα κύρια παραδείγματα συμφωνιών, που έχουν συναφθεί μεταξύ ΕΕ και ΗΠΑ και έχουν ως αντικείμενο τις διασυνοριακές ροές προσωπικών δεδομένων, αποτελούν:[659] [660] η «Συμφωνία PNR μεταξύ της

[657] Βλ. Weber, R. H., & Staiger, D. (2017). *Transatlantic data protection in practice*. Basel. Springer.

[658] Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, No. 187. OECD Publishing.

[659] Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, No. 187. OECD Publishing.

[660] Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 314.

ΕΕ και των ΗΠΑ»[661] [662] και η «Συμφωνία SWIFT μεταξύ της ΕΕ και των ΗΠΑ»[663], στο πλαίσιο των οποίων η διαβίβαση των προσωπικών δεδομένων βασίζεται ουσιαστικά σε αποφάσεις επάρκειας συγκεκριμένης εμβέλειας[664]. Παράλληλα, θα πρέπει να σημειωθεί ότι οι εν λόγω συμφωνίες επιλαμβάνονται μεγάλου όγκου οικονομικών προσωπικών δεδομένων.

9.2.1 Η συμφωνία PNR μεταξύ της ΕΕ και των ΗΠΑ

Καταρχάς, θα πρέπει να αναφερθεί ότι οι καταστάσεις ονομάτων επιβατών (passenger name records, PNR) συνίστανται σε «μη επαληθευμένες πληροφορίες που παρέχονται από τους επιβάτες και συλλέγονται από τους αερομεταφορείς για να επιτρέψουν τις διαδικασίες κράτησης και check-in»[665]. Αναλυτικότερα, στις καταστάσεις ονομάτων επιβατών περιλαμβάνονται δεδομένα όπως: ημερομηνίες ταξιδιού και δρομολόγιο ταξιδιού, πληροφορίες εισιτηρίων, στοιχεία επικοινωνίας, όπως διεύθυνση και αριθμός τηλεφώνου, ταξιδιωτικός πράκτορας, πληροφορίες για την πληρωμή, πληροφορίες για τον αριθμό του καθίσματος και τις αποσκευές[666]. Η διαβίβαση των καταστάσεων ονομάτων επιβατών αποτελεί το αντικείμενο διεθνών συμφωνιών τις οποίες έχει συνάψει η ΕΕ με τρίτες χώρες

[661] Απόφαση 2007/551/ΚΕΠΠΑ/ΔΕΥ του Συμβουλίου της 23ης Ιουλίου 2007 για την υπογραφή, εξ ονόματος της Ευρωπαϊκής Ένωσης, συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής για την επεξεργασία και τη διαβίβαση δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) από τους αερομεταφορείς στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών (DHS) (Συμφωνία 2007 PNR). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32007D0551

[662] Συμφωνία μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης για τη χρήση και τη διαβίβαση των φακέλων ονομάτων επιβατών στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A22012A0811%2801%29

[663]Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής για σκοπούς του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:22010A0727(01)

[664]Βλ. Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford, p. 84.

[665]Βλ. https://ec.europa.eu/home-affairs/policies/law-enforcement-cooperation/passenger-name-record-pnr_el

[666]https://ec.europa.eu/home-affairs/policies/law-enforcement-cooperation/passenger-name-record-pnr_el

(Αυστραλία[667] και ΗΠΑ[668]) και τέθηκαν σε ισχύ στις 1 Ιουνίου 2012[669]. Θα πρέπει να σημειωθεί ότι ο GDPR ισχύει με την επιφύλαξη των εν λόγω διεθνών συμφωνιών (αιτιολογική σκέψη 102 GDPR)[670].

Ο σκοπός της σύναψης της συμφωνίας μεταξύ των ΗΠΑ και της ΕΕ για τη χρήση και τη διαβίβαση των φακέλων ονομάτων επιβατών στο Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ είναι η πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων. Ειδικότερα, όσον αφορά τη συμφωνία για τη χρήση και τη διαβίβαση των φακέλων ονομάτων επιβατών στο Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ του 2012, θα πρέπει να αναφερθεί ότι συνήφθη βάσει της Απόφασης 2007/551/ΚΕΠΠΑ/ΔΕΥ[671] του Συμβουλίου της ΕΕ[672].

Ωστόσο, σε αυτό το σημείο είναι ανάγκη να σημειωθεί ότι αν και η συμφωνία PNR του 2012 είναι η πιο πρόσφατη[673], έχουν διενεργηθεί δύο κοινές αναφορές έκτοτε. Αναλυτικότερα, αυτές είναι η Κοινή ανασκόπηση της Συμφωνίας PNR ΗΠΑ-ΕΕ[674] το 2017 και η Κοινή αξιολόγηση της Συμφωνίας

[667]Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Αυστραλίας για την επεξεργασία και τη διαβίβαση, από τους αερομεταφορείς, δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) προς την Υπηρεσία Τελωνείων και Προστασίας των Συνόρων της Αυστραλίας. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-04/CELEX_22012A0714%2801%29_EL_TXT.pdf

[668]Συμφωνία μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης για τη χρήση και τη διαβίβαση των φακέλων ονομάτων επιβατών στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A22012A0811%2801%29

[669]Βλ. https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/megales_baseisdedomenon/PNR

[670] Συμβούλιο της Ευρώπης. (2018*). Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, σελ. 334 κ. επ.

[671] Απόφαση 2007/551/ΚΕΠΠΑ/ΔΕΥ του Συμβουλίου της 23ης Ιουλίου 2007 για την υπογραφή, εξ ονόματος της Ευρωπαϊκής Ένωσης, συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής για την επεξεργασία και τη διαβίβαση δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) από τους αερομεταφορείς στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών (DHS) (Συμφωνία 2007 PNR). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32007D0551

[672] Ιγγλεζάκης, Ι. (2021). *Δίκαιο Πληροφορικής*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, σελ. 362 κ. επ.

[673]Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 122.

[674]Βλ. https://ec.europa.eu/home-affairs/system/files/2017-01/19012017_pnr_report_en.pdf

PNR ΗΠΑ–ΕΕ[675] το 2021.

Στο σημείο αυτό, αξίζει να αναλυθεί η διαχρονική πορεία των συμφωνιών PNR μεταξύ ΕΕ και ΗΠΑ. Το πρώτο βήμα των συμφωνιών με αντικείμενο τη διαβίβαση των καταστάσεων ονομάτων επιβατών αποτέλεσε η απόφαση[676] της Ευρωπαϊκής Επιτροπής το 2004, η οποία επισφράγισε την ικανοποιητική προστασία των προσωπικών δεδομένων, τα οποία διαβιβάζονταν στην υπηρεσία τελωνείων και προστασίας των συνόρων (Bureau of Customs and Border Protection) των ΗΠΑ. Κατόπιν τούτου, το Συμβούλιο της ΕΕ ενέκρινε[677] τη σύναψη της συμφωνίας PNR. Εν συνεχεία, ωστόσο, το Δικαστήριο της ΕΕ ακύρωσε τις εν λόγω αποφάσεις (του Συμβουλίου και της Επιτροπής) με την απόφαση[678] του στις 30 Μαΐου 2006[679]. Απόρροια της απόφασης του Δικαστηρίου αποτέλεσε η υιοθέτηση συμφωνίας[680] μεταξύ της ΕΕ και των ΗΠΑ, τον Οκτώβριο του 2006, για τα μεταβιβαζόμενα προσωπικά δεδομένα στην υπηρεσία τελωνείων και προστασίας των συνόρων των ΗΠΑ[681] [682].

---

[675]Βλ. https://ec.europa.eu/home-affairs/system/files/2021-01/12012021_commission_report_com-2021-18_en.pdf

[676] 2004/535/ΕΚ:Απόφαση της Επιτροπής, της 14ης Μαΐου 2004, σχετικά με την ικανοποιητική προστασία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στο φάκελο των επιβατών (Passenger Name Record) αεροπορικών μεταφορών ο οποίος διαβιβάζεται στο Bureau of Customs and Border Protection (υπηρεσία τελωνείων και προστασίας των συνόρων) των Ηνωμένων Πολιτειών της Αμερικής [κοινοποιηθείσα υπό τον αριθμό Ε(2004) 1914]. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32004D0535

[677]2004/496/ΕΚ:Απόφαση του Συμβουλίου, της 17ης Μαΐου 2004, για τη σύναψη συμφωνίας μεταξύ της Ευρωπαϊκής Κοινότητας και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση των καταστάσεων με τα ονόματα των επιβατών από τους αερομεταφορείς προς το Υπουργείο Εσωτερικής Ασφάλειας, Υπηρεσία Τελωνείων και Προστασίας των Συνόρων των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32004D0496

[678]C-317/04, C-318/04. Απόφαση του ΔΕΚ (τμήμα μείζονος συνθέσεως) της 30ής Μαΐου 2006, Ευρωπαϊκό Κοινοβούλιο κατά Συμβουλίου της Ευρωπαϊκής Ενώσεως (C-317/04) και Επιτροπή των Ευρωπαϊκών Κοινοτήτων (C-318/04).

[679]Mildebrath, H. European Parliamentary Research Service. (2020). The CJEU judgment in the Schrems II case. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)652073

[680]Απόφαση 2006/729/ΚΕΠΠΑ/ΔΕΥ του Συμβουλίου, της 16ης Οκτωβρίου 2006, για την υπογραφή, εξ ονόματος της Ευρωπαϊκής Ένωσης, συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής για την επεξεργασία και τη διαβίβαση δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) από τους αερομεταφορείς στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32006D0729

[681]ΑΠΔΠΧ. (2007). Ετήσια έκθεση 2006. Εθνικό τυπογραφείο, Αθήνα. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2006.PDF

Θα πρέπει να αναφερθεί ότι η τελευταία συμφωνία[683] PNR μεταξύ ΕΕ και ΗΠΑ του 2012 περιέχει κρίσιμές διατάξεις για τη διασφάλιση της προστασίας των προσωπικών δεδομένων. Πιο συγκεκριμένα, γίνεται ειδική αναφορά στην επεξεργασία των ευαίσθητων προσωπικών δεδομένων στο άρθρο 6, η οποία επιτρέπεται μόνο όταν «διακυβεύεται ή απειλείται σοβαρά η ζωή κάποιου» (άρθρο 6 παρ. 3) και «διαγράφονται οριστικά το αργότερο 30 ημέρες από την τελευταία παραλαβή» (άρθρο 6 παρ. 4 εδ. 1) εκτός και αν υφίσταται σκοπός «ειδικής διερεύνησης, δίωξης ή μέτρων επιβολής» (άρθρο 6 παρ. 4 εδ. 2). Το ζήτημα του ολικού περιορισμού της επεξεργασίας των ευαίσθητων προσωπικών δεδομένων και της απαγόρευσης της διαβίβασής τους στο Υπουργείο Εσωτερικής Ασφαλείας των ΗΠΑ είχε τονιστεί στη Γνωμοδότηση[684] του Ευρωπαίου Επόπτη Προστασίας Δεδομένων. Επιπρόσθετα, αξίζει να σημειωθεί ότι η πρόβλεψη των διαβιβάσεων των δεδομένων σε εθνικές αρχές, εντός των ΗΠΑ, γίνεται στο άρθρο 16 της συμφωνίας, υπό τις προϋποθέσεις που θέτει το άρθρο. Ως προς τις «περαιτέρω» διαβιβάσεις των δεδομένων σε τρίτες χώρες, προβλέπονται στο άρθρο 17 της συμφωνίας και δύνανται να πραγματοποιούνται «με όρους που συνάδουν με την παρούσα συμφωνία» (άρθρο 17 παρ. 1).

Παράλληλα, θα πρέπει να αναφερθεί ότι η ΕΕ εξέδωσε την Οδηγία (ΕΕ) 2016/681[685], σύμφωνα με την οποία η επεξεργασία των δεδομένων πρέπει να πραγματοποιείται «μόνο για τον σκοπό της πρόληψης, ανίχνευσης, διερεύνησης και δίωξης τρομοκρατικών και σοβαρών εγκλημάτων» (άρθρο 1 παρ. 2 της Οδηγίας (ΕΕ) 2016/681), (βλ. υπό 8.7).

---

[682]Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?. In *Institutionalisation beyond the Nation State*. Springer, Cham, (pp. 55-74).

[683]Συμφωνία μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης για τη χρήση και τη διαβίβαση των φακέλων ονομάτων επιβατών στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A22012A0811%2801%29

[684]Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων επί της πρότασης απόφασης του Συμβουλίου σχετικά με τη σύναψη της συμφωνίας μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης για τη χρήση και τη διαβίβαση των φακέλων επιβατών (φάκελοι PNR) στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών (2012/C 35/03). Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/publication/11-12-09_us_pnr_el.pdf

[685] Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016L0681

9.2.2 Η συμφωνία SWIFT μεταξύ της ΕΕ και των ΗΠΑ[686]

(*Δημοσιεύθηκε στα Πρακτικά του 1ου διεπιστημονικού συνεδρίου: «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής)*

Η υπόθεση SWIFT είναι αξιοσημείωτη αφενός για τα θέματα που αναδείχθηκαν μέσα από την ίδια και αφετέρου διότι θέτει την προσοχή στον μετασχηματισμό της ευρωπαϊκής νομοθεσίας υπό το πρίσμα της διασυνοριακής ροής των οικονομικών προσωπικών δεδομένων, τόσο εσωτερικά όσο και εξωτερικά[687]. Επιπλέον, καταδεικνύει τη διαφορετική σημασία της έννοιας της ασφάλειας, όπως αποδίδεται και αξιολογείται από την ΕΕ και τις ΗΠΑ.

Η SWIFT (Society for Worldwide Interbank Financial Telecommunication) είναι μία παγκόσμια συνεταιριστική εταιρία περιορισμένης ευθύνης με έδρα το Βέλγιο, η οποία ως εκ τούτου διέπεται από το βελγικό δίκαιο και χρησιμοποιεί ένα παγκόσμιο σύστημα ανταλλαγής μηνυμάτων προκειμένου να διαβιβάζει πληροφορίες χρηματοοικονομικών συναλλαγών. Αναλυτικότερα, παρέχει υπηρεσίες ανταλλαγής χρηματοπιστωτικών μηνυμάτων που καθιστούν δυνατές τις διεθνείς μεταφορές χρημάτων για πάνω από 11.000 χρηματοπιστωτικά ιδρύματα[688].

Οι καταβολές της συμφωνίας TFTP μεταξύ της ΕΕ και των ΗΠΑ χρονολογούνται στον Ιούνιο του 2006, όταν αναδείχθηκε από τα μέσα ενημέρωσης της Ευρώπης και των ΗΠΑ, η ύπαρξη του Προγράμματος Ανίχνευσης της Χρηματοδότησης της Τρομοκρατίας (Terrorist Finance Tracking Program, TFTP), που θέσπισε η κυβέρνηση των ΗΠΑ, χάρη στο οποίο κατέστη δυνατό οι αρχές των ΗΠΑ να αποκτήσουν πρόσβαση σε ένα τμήμα των οικονομικών δεδομένων Ευρωπαίων πολιτών που συγκεντρώνει η SWIFT[689]. Ο σκοπός ήταν να προσδιορίσουν, να παρακολουθήσουν και να ταυτοποιήσουν τους

---

[686] Η παρούσα ενότητα του κεφαλαίου αποτελεί μέρος της εισήγησης που δημοσιεύθηκε στα Πρακτικά του 1ου διεπιστημονικού συνεδρίου: «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, υπό τον τίτλο: Ρίζου, Σ. (2019). Διασυνοριακή ροή οικονομικών δεδομένων: Η Συμφωνία SWIFT σε: Αλεξανδροπούλου, Ε., Δαλακούρας, Θ., Μαστροκώστας, Χ. (2019). Πρακτικά 1ου διεπιστημονικού συνεδρίου «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής. Νομική Σχολή ΔΠΘ. Κομοτηνή 25-26 Μαΐου 2018. εκδ. Νομική Βιβλιοθήκη, Αθήνα.

[687] De Goede, M. (2012). The SWIFT affair and the global politics of European security. *JCMS: Journal of Common Market Studies*, *50*(2), 214-230.

[688] Σύμφωνα με τον ιστότοπο της SWIFT: https://www.swift.com/about-us/discover-swift

[689] Μυλώση, Μ. (2015). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία.σελ. 266 επ.

τρομοκράτες και τα δίκτυα στα οποία εντάσσονται διαμέσου των ροών των χρημάτων τους[690]. Παρά το γεγονός ότι η ύπαρξη του προγράμματος TFTP δημοσιοποιήθηκε από τους New York Times[691] τον Ιούνιο του 2006, το πρόγραμμα έχει την απαρχή του τον Οκτώβριο του 2001[692], ως απόρροια των επιθέσεων της 11ης Σεπτεμβρίου 2001. Ειδικότερα, το Υπουργείο Οικονομικών των ΗΠΑ που λειτουργούσε μυστικά το πρόγραμμα TFTP από το 2001 σε συνεργασία με την Κεντρική Υπηρεσία Πληροφοριών των ΗΠΑ (CIA), είχε συλλέξει και αναλύσει μεγάλο όγκο δεδομένων από τη SWIFT, τα οποία αποθηκεύονταν σε ένα αντίγραφο βάσης δεδομένων (mirror database)[693]. Η διαβίβαση αυτή κατέστη εφικτή μέσω του κέντρου επεξεργασίας δεδομένων που διατηρούσε η SWIFT στις ΗΠΑ, όπου υπήρχαν αντίγραφα όλων των συναλλαγών αποθηκευμένα για το διάστημα 124 ημερών. Το Υπουργείο Οικονομικών των ΗΠΑ εξέδωσε κλήσεις προς το κέντρο αυτό, αποκτώντας ακολούθως πρόσβαση σε δεδομένα παγκόσμιας κλίμακας, περιλαμβανομένων, μεταξύ άλλων, αυτών των Ευρωπαίων πολιτών[694].

Ο αντίκτυπος της ευρείας γνωστοποίησης του προγράμματος TFTP στην Ευρωπαϊκή Ένωση πυροδότησε σειρά ενεργειών και διαβουλεύσεων τα επόμενα έτη. Εν πρώτοις θα πρέπει να τονιστεί ότι η Ευρωπαϊκή Κεντρική Τράπεζα ήταν μία από τις κύριες εποπτικές αρχές της SWIFT[695]. Το Ευρωπαϊκό Κοινοβούλιο ενέκρινε ψήφισμα τον Ιούλιο του 2006 με το οποίο εξέφρασε τις ανησυχίες του για το πρόγραμμα TFTP και απέρριψε τη μη διαφάνεια κάθε πράξης που

[690] Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?. In *Institutionalisation beyond the Nation State*. Springer, Cham, (pp. 55-74).

[691] Lichtblau, E., & Risen, J. (2006). Bank data is sifted by US in secret to block terror. *New York Times*, *23*, 66-205.

[692] De Goede, M. (2012). The SWIFT affair and the global politics of European security. *JCMS: Journal of Common Market Studies*, *50*(2), 214-230.

[693] Αναφορά για τον έλεγχο της εφαρμογής της συμφωνίας TFTP, ο οποίος πραγματοποιήθηκε το Νοέμβριο του 2010 από την Κοινή Εποπτική Αρχή της Europol. Διαθέσιμο στο: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/int/20110322_jsb_tftp_inspection.pdf

[694] De Goede, M. (2012). The SWIFT affair and the global politics of European security. *JCMS: Journal of Common Market Studies*, *50*(2), 214-230.

[695] Article 29 Working Party. (2006). "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)". Διαθέσιμο στο: http://www.dataprotection.ro/servlet/ViewDocument?id=234

αφορούσε την προστασία της ιδιωτικής ζωής των Ευρωπαίων πολιτών[696]. Παράλληλα, σύμφωνα με τη γνώμη της βελγικής αρχής προστασίας προσωπικών δεδομένων, η μεταφορά δεδομένων από τις υπηρεσίες SWIFT παραβίασε την εθνική νομοθεσία του Βελγίου, ως χώρα εφαρμοστέου δικαίου για τη SWIFT ως προς τη διαβίβαση των δεδομένων σε τρίτες χώρες. Αναλυτικότερα, σύμφωνα με τη νομοθεσία του Βελγίου για την προστασία προσωπικών δεδομένων, η SWIFT δεν νομιμοποιούνταν να διαβιβάζει στις ΗΠΑ προσωπικά δεδομένα, διότι οι ΗΠΑ δεν παρείχαν ικανοποιητικό επίπεδο προστασίας των προσωπικών δεδομένων, προϋπόθεση του άρθρου 25 της Οδηγίας 95/46/ΕΚ για να καταστεί δυνατή η διαβίβαση δεδομένων σε τρίτες χώρες. Επιπλέον, η SWIFT όφειλε να ενημερώσει τους χρήστες των υπηρεσιών, οι οποίοι εν προκειμένω ήταν τα εκάστοτε χρηματοπιστωτικά ιδρύματα, για το γεγονός της διαβίβασης στις ΗΠΑ, προσωπικών δεδομένων και της πρόσβασης σ' αυτά από το Υπουργείο Οικονομικών των ΗΠΑ. Τα χρηματοπιστωτικά ιδρύματα όφειλαν ακόμη να ενημερώσουν τους πελάτες τους που χρησιμοποιούσαν τις υπηρεσίες του SWIFT[697]. Παράλληλα, σύμφωνα με τη Γνώμη της ομάδας εργασίας για την προστασία δεδομένων, η οποία συστάθηκε από το άρθρο 29 της οδηγίας 95/46/ΕΚ, οι διαβιβάσεις οι οποίες πραγματοποιήθηκαν στο πλαίσιο του προγράμματος ήταν ασύμβατες με τα άρθρα της Οδηγίας 95/46/ΕΚ[698].

Η πρόσβαση στα οικονομικά στοιχεία της SWIFT από το Υπουργείο Οικονομικών των ΗΠΑ συνεχίστηκε στο πλαίσιο αυτού του καθεστώτος, έως ότου η SWIFT ανακοίνωσε τον Οκτώβριο του 2007, την αναδιάρθρωση της δομής του ηλεκτρονικού συστήματος ανταλλαγής μηνυμάτων, βάσει του οποίου διαβιβάζονταν τα οικονομικά δεδομένα που προέρχονταν από την ΕΕ, προκειμένου η αποθήκευση των δεδομένων αυτών να λαμβάνει χώρα αποκλειστικά στην Ευρώπη. Ως αποτέλεσμα της εν λόγω ανακοίνωσης, κατέστη απαραίτητη η έναρξη της διαπραγμάτευσης για την επίτευξη συμφωνίας μεταξύ της ΕΕ και των ΗΠΑ, η οποία να επιτρέπει στο Υπουργείο Οικονομικών των

[696] Ψήφισμα της 6ης Ιουλίου 2006 του Ευρωπαϊκού Κοινοβουλίου σχετικά με την παρακολούθηση των δεδομένων τραπεζικών εντολών με το σύστημα SWIFT από τις μυστικές υπηρεσίες των ΗΠΑ, Διαθέσιμο στο: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0317+0+DOC+XML+V0//EL&language=EL

[697] Μυλώση, Μ. (2015). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία. σελ. 266 επ.

[698] Article 29 Working Party. (2006). "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)". Διαθέσιμο στο: http://www.dataprotection.ro/servlet/ViewDocument?id=234

ΗΠΑ τη διαβίβαση των οικονομικών στοιχείων μέσω της διεξαγωγής διοικητικών κλήσεων στη SWIFT[699].

Στις 30 Νοεμβρίου 2009, μία ημέρα πριν από την έναρξη ισχύος της Συνθήκης της Λισαβόνας, εγκρίθηκε από το Ευρωπαϊκό Συμβούλιο η Ενδιάμεση συμφωνία TFTP μεταξύ της ΕΕ και των ΗΠΑ. Θα πρέπει να σημειωθεί πως μετά την έναρξη ισχύος της Συνθήκης της Λισαβόνας την 1η Δεκεμβρίου 2009, απαιτείται η έγκριση του Ευρωπαϊκού Κοινοβουλίου για σύναψη της συμφωνίας από το Συμβούλιο της ΕΕ σύμφωνα με τη διαδικασία που προβλέπει το άρθρο 218 ΣΛΕΕ, διότι αφορά την κοινή εξωτερική πολιτική της ΕΕ και την πολιτική ασφάλειας. Στις 11 Φεβρουαρίου 2010, κατόπιν σύστασης της κοινοβουλευτικής επιτροπής LIBE, το Ευρωπαϊκό Κοινοβούλιο καταψήφισε τη σύναψη ενδιάμεσης συμφωνίας TFTP[700]. Μετά την απόρριψη της Ενδιάμεσης Συμφωνίας TFTP από το Ευρωπαϊκό Κοινοβούλιο, και κατόπιν δεύτερου γύρου διαπραγματεύσεων, η νέα συμφωνία TFTP ολοκληρώθηκε μετά την υπερψήφισή της από το ΕΚ την 8η Ιουλίου 2010[701].

Η συμφωνία μεταξύ της ΕΕ και των ΗΠΑ, σχετικά με την επεξεργασία και τη διαβίβαση στοιχείων μηνυμάτων χρηματοοικονομικής φύσεως από την Ευρωπαϊκή Ένωση στις ΗΠΑ, για σκοπούς του Προγράμματος Παρακολούθησης της Χρηματοδότησης της Τρομοκρατίας (TFTP) τέθηκε σε ισχύ την 1η Αυγούστου 2010, όπως ορίζει το κείμενο της συμφωνίας. Συλλήβδην, καθορίζει τον σκοπό της μεταφοράς των οικονομικών δεδομένων και τις διαδικασίες που πρέπει να τηρεί το Υπουργείο Οικονομικών των ΗΠΑ για να αποκτήσει πρόσβαση σε αυτά. Αναλυτικότερα, ορίζει τη φύση των δεδομένων, τη χρονική περίοδο διατήρησής τους, τις διασφαλίσεις που ισχύουν για την επεξεργασία των δεδομένων καθώς και τα δικαιώματα του υποκειμένου των δεδομένων. Προβλέπει κοινή έκθεση σχετικά με το πρόγραμμα TFTP, κοινές αναθεωρήσεις της

[699] Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?. In *Institutionalisation beyond the Nation State*. Springer, Cham, (pp. 55-74).

[700]European Parliament legislative resolution of 11 February 2010 on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme (05305/1/2010 REV 1 — C7-0004/2010 — 2009/0190(NLE)) P7_TA(2010)0029.

[701]Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής για σκοπούς του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:22010A0727(01)

συμφωνίας, διαβουλεύσεις μεταξύ των δύο μερών και τη θέσπιση ανεξάρτητης εποπτείας ως προς τη συμμόρφωση με τη συμφωνία.[702]

Ως προς τη φύση των δεδομένων στα οποία αναφέρεται η συμφωνία TFTP, κατά το άρθρο 5 παρ. 7 της συμφωνίας, δύνανται να συμπεριλαμβάνουν πληροφορίες για τον προσδιορισμό του εντολέα και/ή του αποδέκτη της συναλλαγής, μεταξύ των οποίων το όνομα, ο αριθμός λογαριασμού, η διεύθυνση και ο εθνικός αριθμός ταυτότητας. Ακόμη, δύνανται τα διαβιβαζόμενα δεδομένα να αποτελούν «ευαίσθητα» δεδομένα (ήτοι, προσωπικά δεδομένα που παρέχουν πληροφορίες για τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις και την υγεία ή τη σεξουαλική ζωή)[703], τα οποία πρέπει να προστατεύονται από τις αρχές των ΗΠΑ, επιδεικνύοντας πλήρη σεβασμό και λαμβάνοντας δεόντως υπόψη τον ιδιαίτερα ευαίσθητο χαρακτήρα τους[704].

Το άρθρο 4 της συμφωνίας TFTP μεταξύ της ΕΕ και των ΗΠΑ παρουσιάζει αναλυτικά, προκειμένου να διασφαλίζεται η νομιμότητα, τη διαδικασία σύμφωνα με την οποία υποβάλλονται οι αιτήσεις για πρόσβαση στα δεδομένα από το Υπουργείο Οικονομικών των ΗΠΑ[705]. Πιο συγκεκριμένα, το Υπουργείο Οικονομικών των ΗΠΑ οφείλει να αποστείλει αίτημα για την πρόσβαση στα δεδομένα της SWIFT, το οποίο πρέπει να εγκριθεί από την Europol για να λάβει νομική ισχύ, ώστε να νομιμοποιηθεί η διαβίβαση των δεδομένων. Τα αιτήματα περιγράφουν όσο το δυνατόν σαφέστερα τα δεδομένα των οποίων η διερεύνηση καθίσταται αναγκαία για την πρόληψη, διερεύνηση, ανίχνευση ή δίωξη της τρομοκρατίας ή της χρηματοδότησής της. Παράλληλα, το αίτημα για την πρόσβαση στα δεδομένα πρέπει να είναι αφενός όσο το δυνατόν πιο περιορισμένο, ώστε να περιορίζεται ο όγκος των ζητουμένων δεδομένων στα αναγκαία, ικανοποιώντας την αρχή της αναλογικότητας, και αφετέρου τεκμηριωμένο. Επί του πρακτέου, θα πρέπει να σημειωθεί πως, σύμφωνα με τους ελέγχους που πραγματοποιεί η Κοινή Εποπτική Αρχή (ΚΕΑ) της Europol, το θέμα της ορθής αξιολόγησης και έγκρισης των αιτημάτων των αμερικανικών

[702] Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?. In *Institutionalisation beyond the Nation State*. Springer, Cham, (pp. 55-74).

[703] Möller, C. (2017). *The Evolution of Data Protection and Privacy in the Public Security Context-An Institutional Analysis of Three EU Data Retention and Access Regimes* (Doctoral dissertation, Queen Mary University of London).

[704] Άρθρο 5 παρ.7 της συμφωνίας (2010/412/ΕΕ)

[705] Συμφωνία (2010/412/ΕΕ)

αρχών εντοπίζεται κυρίως στην αοριστία ως προς την αναγκαιότητα των αιτούμενων διαβιβάσεων δεδομένων[706].

Το άρθρο 5 της συμφωνίας προβλέπει τις εγγυήσεις που διέπουν την επεξεργασία των δεδομένων από τις αρχές των ΗΠΑ, κατόπιν της εγκρίσεως από την Europol. Καταρχάς, η επεξεργασία των δεδομένων θα λαμβάνει χώρα αποκλειστικά για τον σκοπό της πρόληψης, της διερεύνησης, της ανίχνευσης της δίωξης ή της χρηματοδότησής της τρομοκρατίας. Παράλληλα, το πρόγραμμα TFTP δεν δύναται να προχωρήσει σε εξόρυξη δεδομένων ή σε τυχόν άλλους τύπους αλγοριθμικής ή αυτόματης ανάλυσης προφίλ ή ηλεκτρονικού φιλτραρίσματος. Συλλήβδην, τα πρότυπα ασφάλειας διατήρησης των δεδομένων, όπως η ασφαλής αποθήκευση, η περιορισμένη πρόσβαση σε αυτά, η προστασία από χειραγώγηση και αλλοίωση, προβλέπονται στο άρθρο 5[707]. Ειδικότερα, ως προς τη διατήρηση της ασφάλειας και της ακεραιότητας των δεδομένων, απαγορεύεται η διασύνδεση των δεδομένων με καμία άλλη βάση δεδομένων.

Η συμφωνία ενισχύει σημαντικά την προστασία των προσωπικών δεδομένων, εγγυώμενη τη διαφάνεια της επεξεργασίας, καθώς επίσης και τα δικαιώματα πρόσβασης, διόρθωσης και διαγραφής των ανακριβών δεδομένων. Στο πλαίσιο της συμφωνίας TFTP, τα δεδομένα που διαβιβάζονται στις αρχές των ΗΠΑ και αφορούν διατραπεζικές συναλλαγές από λογαριασμούς Ευρωπαίων πολιτών, τυγχάνουν προστασίας από τις προβλεπόμενες διατάξεις των άρθρων 15 και 16[708]. Συγκεκριμένα, το άρθρο 15 της συμφωνίας προβλέπει τη δυνατότητα του υποκειμένου των δεδομένων να ζητήσει πρόσβαση στα δεδομένα του που έχουν τύχει επεξεργασίας στο πλαίσιο της συμφωνίας, ενώ το άρθρο 16 προβλέπει τη δυνατότητα του υποκειμένου να ζητήσει τη διόρθωση, τη διαγραφή ή το κλείδωμα των δεδομένων προσωπικού χαρακτήρα που είναι ανακριβή ή που υποβάλλονται σε επεξεργασία κατά παράβαση της συμφωνίας. Τα ανωτέρω

[706] Αναφορά για τον έλεγχο της εφαρμογής της συμφωνίας TFTP, ο οποίος πραγματοποιήθηκε το Νοέμβριο του 2010 από την Κοινή Εποπτική Αρχή της Europol. Διαθέσιμο στο: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/int/20110322_jsb_tftp_inspection.pdf

[707] Möller, C. (2017). *The Evolution of Data Protection and Privacy in the Public Security Context-An Institutional Analysis of Three EU Data Retention and Access Regimes* (Doctoral dissertation, Queen Mary University of London).

[708] Βλ.http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/08B7FE59EA0CF68BC225820C0021E80A?OpenDocument&highlight=SWIFT

δικαιώματα ασκούνται ενώπιον του Υπουργείου Οικονομικών των ΗΠΑ, μέσω της εκάστοτε εθνικής Αρχής Προστασίας Δεδομένων[709].

Το άρθρο 13 της συμφωνίας προβλέπει κοινές επανεξετάσεις, σε τακτά διαστήματα, των διατάξεων περί εγγυήσεων, ελέγχων και αμοιβαιότητας, οι οποίες διενεργούνται από ομάδες επανεξέτασης της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών, συμπεριλαμβανομένης της Ευρωπαϊκής Επιτροπής, του Υπουργείου Οικονομικών των ΗΠΑ και εκπροσώπων δύο αρχών προστασίας δεδομένων από κράτη μέλη της ΕΕ. Στις ομάδες ενδέχεται να συμμετέχουν και εμπειρογνώμονες σε θέματα ασφάλειας και προστασίας δεδομένων, καθώς και άτομα με δικαστική πείρα. Σύμφωνα με την τελευταία και τέταρτη κατά σειρά Έκθεση της Ευρωπαϊκής Επιτροπής για την από κοινού επανεξέταση της εφαρμογής της συμφωνίας που πραγματοποιήθηκε στις 19 Ιανουαρίου 2017, η Επιτροπή εξέφρασε την ικανοποίησή της από την ορθή εφαρμογή της συμφωνίας, των ελέγχων της και των εγγυήσεων που παρέχει, όσον αφορά τη διαβίβαση των δεδομένων[710].

Παράλληλα, τέθηκε σε ενωσιακό επίπεδο το ζήτημα της σύστασης ενός Ευρωπαϊκού Συστήματος Παρακολούθησης της Χρηματοδότησης της Τρομοκρατίας, τον Ιούλιο του 2011. Η Επιτροπή της ΕΕ ενέκρινε ανακοίνωση[711], όσον αφορά τη δημιουργία ενός Ευρωπαϊκού Συστήματος Παρακολούθησης της Χρηματοδότησης της Τρομοκρατίας (TFTS), για το οποίο το Κοινοβούλιο εξέφρασε αμφιβολίες. Τον Νοέμβριο του 2013, η Επιτροπή ανακοίνωσε ότι στο εν λόγω στάδιο δεν είχε κρίνει σκόπιμη τη δημιουργία ενός Ευρωπαϊκού TFTS[712].

Όσον αφορά τις θεσμικές εξελίξεις στην υπόθεση SWIFT, σε ενωσιακό επίπεδο, το Ευρωπαϊκό Κοινοβούλιο εξέδωσε το Ψήφισμα 2013/2831, με το οποίο αιτήθηκε την προσωρινή αναστολή της συμφωνίας SWIFT, προκειμένου να διαπιστωθεί αφενός η ενδεχόμενη μη εξουσιοδοτημένη πρόσβαση σε οικονομικά δεδομένα, υπερβαίνοντας τις εξουσίες που προβλέπει η συμφωνία, και αφετέρου

[709] ΑΠΔΠΧ. Συμφωνία μεταξύ ΕΕ και ΗΠΑ σχετικά με τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων. Διαθέσιμο στο : https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/megales_baseisdedomenon/TFTP

[710] Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την από κοινού επανεξέταση της εφαρμογής της συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής για τους σκοπούς του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας, COM/2017/031 final, Διαθέσιμο στο: http://ec.europa.eu/transparency/regdoc/rep/1/2013/EL/1-2013-842-EL-F1-1.Pdf

[711] Βλ. http://europa.eu/rapid/press-release_IP-11-877_el.htm

[712] Βλ. http://europa.eu/rapid/press-release_IP-13-1160_el.htm

η ανάλυση των διαδικασιών που προβλέπονται από τη συμφωνία και ο εντοπισμός της λύσης για την προσήκουσα εφαρμογή αυτών[713]. Από την άλλη μεριά, ως απάντηση για τις μη εξουσιοδοτημένες εξουσίες των αμερικανικών υπηρεσιών, το Κογκρέσο των ΗΠΑ θέσπισε τον «Νόμο για την Ελευθερία των Πληροφοριών» (US Freedom Act), ο οποίος τέθηκε σε εφαρμογή στις 2 Ιουνίου 2015[714]. Ο σκοπός αυτού του νόμου είναι να τερματίσει τη μαζική συλλογή δεδομένων των Αμερικανών από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ (National Security Agency, NSA)[715]. Ο US Freedom Act τροποποίησε τον American Patriot Act που αφορά την ενίσχυση της εθνικής ασφάλειας ενάντια στην τρομοκρατία και τον νόμο για την Παρακολούθηση των Εξωτερικών Πληροφοριών (Foreign Intelligence Surveillance Act, FISA)[716].

Αναμφισβήτητα, η τελική συμφωνία SWIFT, όπως ισχύει επί του παρόντος νομιμοποίησε και επαναπροσδιόρισε το πρόγραμμα TFTP, από ένα μυστικό και προσωρινό μέτρο σε ένα διαρκές και θεσμοθετημένο διατλαντικό πρόγραμμα διεθνούς ασφάλειας, όπως αρμόζει σε μία συμφωνία, η οποία αφορά την ευρεία πρόσβαση και ανάλυση χρηματοοικονομικών δεδομένων πολιτών, στο πλαίσιο της πάταξης της τρομοκρατίας με εφαλτήριο όχημα τη χρηματοδότηση της[717].

9.2.3 Από τη Συμφωνία του ασφαλούς λιμένα ΕΕ-ΗΠΑ στην Ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ[718]

(*Δημοσιεύθηκε στα Πρακτικά του 1ου διεπιστημονικού συνεδρίου: «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής*)

[713]Ευρωπαϊκό Κοινοβούλιο. Ψήφισμα 2013/2831 σχετικά με την αναστολή της συμφωνίας TFTP ως αποτέλεσμα της παρακολούθησης εκ μέρους της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ.

[714]Βλ. https://www.congress.gov/bill/114th-congress/house-bill/2048/text

[715]Για το National Security Agency/Central Security Service (NSA/CSS), Βλ. https://www.nsa.gov/about/faqs/

[716]Raducu, I. (2014). Reflections Upon the Interaction between Domestic and European Personal Data Protection Legislation. *University of Luxembourg Law Working Paper*, (2014-05).

[717]De Goede, M. (2012). The SWIFT affair and the global politics of European security. *JCMS: Journal of Common Market Studies*, *50*(2), 214-230.

[718]Η παρούσα ενότητα του κεφαλαίου αποτελεί μέρος της εισήγησης που δημοσιεύθηκε στα Πρακτικά του 1ου διεπιστημονικού συνεδρίου: «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, υπό τον τίτλο: Ρίζου Σ. (2019). Διασυνοριακή ροή οικονομικών δεδομένων: Η Συμφωνία SWIFT σε: Αλεξανδροπούλου, Ε., Δαλακούρας, Θ., Μαστροκώστας, Χ. (2019). Πρακτικά 1ου διεπιστημονικού συνεδρίου «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής. Νομική Σχολή ΔΠΘ. Κομοτηνή 25-26 Μαΐου 2018. εκδ. Νομική Βιβλιοθήκη, Αθήνα.

Οι αρχές του «ασφαλούς λιμένα» ήταν μια συμφωνία, η οποία συνήφθη για την προστασία των δεδομένων των πολιτών της ΕΟΧ, τα οποία μεταφέρονταν στις Ηνωμένες Πολιτείες από εταιρείες των ΗΠΑ. Οι εταιρείες των ΗΠΑ που ήθελαν να συμμετάσχουν στο καθεστώς «Safe Harbor» πιστοποιούσαν ότι θα προστατεύουν τα δεδομένα τα οποία μεταβιβάζονται μεταξύ της ΕΕ και των Ηνωμένων Πολιτειών[719]. Οι αρχές του «ασφαλούς λιμένα» αποτυπώνονται στην Απόφαση 2000/520[720] της Επιτροπής της ΕΕ, κατά την οποία το καθεστώς αυτό εξασφαλίζει το κριτήριο του ικανοποιητικού επιπέδου προστασίας των προσωπικών δεδομένων. Αναλυτικότερα, η εν λόγω απόφαση εξεδόθη στο πλαίσιο της αρμοδιότητας της Ευρωπαϊκής Επιτροπής για αναγνώριση των χωρών με επαρκές επίπεδο προστασίας των προσωπικών δεδομένων κατά το άρθρο 25 παρ. 6 της Οδηγίας 95/46/ΕΚ. Εκτός των συμφωνιών «Safe Harbor», η διασυνοριακή ροή δεδομένων μεταξύ ΕΕ και ΗΠΑ επιτυγχανόταν σε ρυθμιστικό επίπεδο, διαμέσου των Model Contractual Clauses, σύμφωνα με τις οποίες διαβιβάζονταν επί του πρακτέου τα δεδομένα των παγκόσμιων τεχνολογικών εταιρειών[721] και των Binding Corporate Rules που θεσπίστηκαν με τη Σύσταση 1/2007[722]. Η απόφαση 2000/520 της Ευρωπαϊκής Επιτροπής ακυρώθηκε από το Δικαστήριο της ΕΕ στις 6.10.2015 (υπόθ. C-362/2014, Schrems I)[723] [724] [725]. Ως εκ τούτου, τον Οκτώβριο του 2015, για λόγους ασυμβατότητας προς το νομικό ευρωπαϊκό πλαίσιο, μετά και την αποκάλυψη μαζικής επεξεργασίας των διαβιβαζόμενων στις ΗΠΑ δεδομένων από τις Υπηρεσίες Ασφαλείας των ΗΠΑ, η

[719]Hall, H. K. (2018). Restoring dignity and harmony to united states-european union data protection regulation. *Communication Law and Policy, 23*(2), 125-157.

[720]2000/520/ΕΚ: Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ [κοινοποιηθείσα υπό τον αριθμό Ε(2000) 2441]. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:32000D0520

[721] Robinson, D. (2016). Facebook data transfers threatened by EU ruling. *Financial Times*. Διαθέσιμο στο: https://www.ft.com/content/8fe7c850-226f-11e6-9d4d-c11776a5124d

[722]Τάσσης, Σ. (2015). ΔΕΕ υπόθ. C-362/2014, απόφ. της 6.10.2015 [Διασυνοριακή ροή δεδομένων] (σημ.). *ΔΙΜΕΕ 3*, 498-512.

[723]C-362/14. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015, Maximillian Schrems κατά Data Protection Commissioner.

[724]Βλ. Τάσσης, Σ. (2015). ΔΕΕ υπόθ. C-362/2014, απόφ. της 6.10.2015 [Διασυνοριακή ροή δεδομένων] (σημ.). *ΔΙΜΕΕ 3*, 498-512.

[725]Βλ. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων). *ΔΙΜΕΕ, 1*, 12-24.

ΕΕ διαπραγματεύτηκε με τις ΗΠΑ νέους αυστηρότερους κανόνες προστασίας των διαβιβαζόμενων προσωπικών δεδομένων στις ΗΠΑ.

Την 2.2.2016 η Ευρωπαϊκή Επιτροπή συμφώνησε με τις ΗΠΑ ένα νέο ρυθμιστικό πλαίσιο για τη διατλαντική ροή δεδομένων με προστατευτικότερους κανόνες για τα διαβιβαζόμενα στις ΗΠΑ δεδομένα. Η 2016/1250 Απόφαση της Επιτροπής της 12ης Ιουλίου του 2016 έθεσε σε εφαρμογή την «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα»[726], η οποία αντικατοπτρίζει τις απαιτήσεις που έθεσε το Δικαστήριο της ΕΕ στην απόφασή του τον Οκτώβριο του 2015. Το καθεστώς της «EU-U.S. Privacy Shield», όπως και το προηγούμενο καθεστώς του «ασφαλούς λιμένα», βασιζόταν σε ένα σύστημα αυτοπιστοποίησης με το οποίο οι αμερικανικές εταιρίες δεσμεύονται από ένα σύνολο αρχών προστασίας της ιδιωτικής ζωής. Ωστόσο, σε αντίθεση με το «Safe Harbor», που περιείχε μία γενική εξαίρεση για λόγους εθνικής ασφάλειας, η «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» προέβλεπε ρητά στο κεφάλαιο 3 την πρόσβαση και τη χρήση προσωπικών δεδομένων από τις δημόσιες Αρχές των ΗΠΑ, που μεταφέρονται βάσει της συμφωνίας για σκοπούς εθνικής ασφάλειας, επιβολής του νόμου και άλλους σκοπούς δημόσιου συμφέροντος[727]. Από την 1η Αυγούστου 2016, οι εταιρείες μπορούσαν να προσχωρούν στην «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» με το Υπουργείο Εμπορίου των ΗΠΑ να ελέγχει εάν οι πολιτικές τους στον τομέα της προστασίας της ιδιωτικότητας συνάδουν με τα υψηλά πρότυπα προστασίας των δεδομένων που απαιτούνται από αυτήν[728], μέχρι την ακύρωση της «Ασπίδας προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» από το ΔΕΕ στις 16 Ιουλίου 2020 στην απόφαση Schrems II[729].

[726] Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ [κοινοποιηθείσα υπό τον αριθμό C(2016) 4176]. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016D1250

[727] Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?. In *Institutionalisation beyond the Nation State*. Springer, Cham, (pp. 55-74).

[728] Milt, K. (2017). Personal data protection. Fact Sheets on the European Union. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/search.html?authors=28691

[729] C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

9.2.4 Η ακυρότητα της Ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ

Το ΔΕΕ εξέτασε, στην απόφαση Schrems II[730], το κύρος της εκτελεστικής απόφασης (ΕΕ) 2016/1250 της Επιτροπής «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα». Πιο συγκεκριμένα, το ΔΕΕ αποφάνθηκε ότι οι επιταγές της εθνικής νομοθεσίας των ΗΠΑ, και ειδικότερα ορισμένα προγράμματα (όπως το PRISM και το UPSTREAM[731]), τα οποία επιτρέπουν την πρόσβαση των αμερικανικών δημοσίων αρχών σε προσωπικά δεδομένα για σκοπούς εθνικής ασφάλειας, έχουν ως αποτέλεσμα τη δημιουργία περιορισμών στην προστασία των προσωπικών δεδομένων που «δεν οριοθετούνται με τέτοιον τρόπο ώστε να ανταποκρίνονται σε απαιτήσεις ουσιαστικά ισοδύναμες με εκείνες που επιβάλλει το δίκαιο της Ένωσης» (σκέψη 185 της απόφασης Schrems II). Αναλυτικότερα, στην απόφαση διαπιστώνεται ότι στοιχεία των διατάξεων της νομοθεσίας των ΗΠΑ δεν συνάδουν με την αρχή της αναλογικότητας, υπό το πρίσμα της νομοθεσίας της ΕΕ (σκέψη 184 της απόφασης Schrems II). Η απόφαση υπογραμμίζει την ανάγκη ύπαρξης συγκεκριμένων κανόνων νόμιμης διαβίβασης των δεδομένων, στο πλαίσιο αυτό, προκειμένου να μην πραγματοποιούνται αδιάκριτα διαβιβάσεις δεδομένων.

Παράλληλα, το ΔΕΕ διαπίστωσε ότι η αμερικανική νομοθεσία δεν παρείχε «στα υποκείμενα των δεδομένων εκτελεστά δικαιώματα τα οποία να μπορούν να προβληθούν έναντι των αμερικανικών αρχών ενώπιον των δικαστηρίων» (σκέψη 181 της απόφασης Schrems II). Η απόφαση για την ακύρωση της «Ασπίδας προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα», η οποία βασίστηκε στο ουσιαστικά μη ισοδύναμο επίπεδο προστασίας των δεδομένων με εκείνο της ΕΕ, κατέστησε αδύνατες τις διασυνοριακές διαβιβάσεις προσωπικών δεδομένων βάσει αυτού του πλαισίου, επιτάσσοντας τη μεταστροφή των εξαγωγών των δεδομένων στα εργαλεία του άρθρου 46 και 49 του GDPR[732].

[730] C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

[731] Mildebrath, H. European Parliamentary Research Service. (2020). The CJEU judgment in the Schrems II case. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)652073

[732] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συχνές ερωτήσεις σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C- 311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximillian Schrems». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_el

Από την πλευρά τους οι ΗΠΑ, θα πρέπει να αναφερθεί ότι εξέδωσαν μία λευκή βίβλο[733] το Σεπτέμβριο του 2020 με τίτλο: «Πληροφορίες σχετικά με τις διασφαλίσεις της ιδιωτικότητας των ΗΠΑ σχετικά με τις SCC και άλλες νομικές βάσεις των διαβιβάσεων μεταξύ ΕΕ-Η.Π.Α. μετά τη Schrems II (Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II)», με σκοπό την καθοδήγηση των οργανισμών μετά την παύση της «Ασπίδας προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα», αναφέροντας ότι «περισσότερες από 5.300 εταιρείες» βασίζονταν σε αυτή.

Επιπρόσθετα, στο σημείο αυτό, επιβάλλεται να αναφερθεί η σχέση μεταξύ της αυστηροποίησης του εργαλείου διαβίβασης των «κατάλληλων εγγυήσεων» και της διαπίστωσης της μη εξασφάλισης ουσιαστικά ισοδύναμου επιπέδου προστασίας από τη νομοθεσία των ΗΠΑ[734]. Το ζήτημα για την περίπτωση των ΗΠΑ προκύπτει επειδή και τα δύο κύρια σκέλη της απόφασης Schrems II αφορούν τις ΗΠΑ ως τρίτη χώρα στο πλαίσιο των διασυνοριακών διαβιβάσεων. Πιο συγκεκριμένα, εφόσον η σκέψη 133 της απόφασης επιτάσσει τη λήψη πρόσθετων μέτρων, προκειμένου να επιτυγχάνεται η τήρηση του ισοδύναμου επιπέδου προστασίας των δεδομένων, όταν απαιτείται όπου εφαρμόζονται «τυποποιημένες ρήτρες προστασίας δεδομένων» και οι ΗΠΑ δεν παρέχουν το ισοδύναμο επίπεδο προστασίας, τότε θα πρέπει να αξιολογηθεί η κάθε διαβίβαση με την υιοθέτηση πρόσθετων μέτρων[735]. Η ενίσχυση της προστασίας, ως προς τις «τυποποιημένες ρήτρες προστασίας δεδομένων», αφορά όλα τα εργαλεία των «κατάλληλων εγγυήσεων» του άρθρου 46[736].

---

[733] Βλ. United States Department of Commerce. (2020). "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II". Διαθέσιμο στο: https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

[734] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συχνές ερωτήσεις σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C- 311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximillian Schrems». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_el

[735] Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συχνές ερωτήσεις σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C- 311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximillian Schrems». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_el

[736] Kuner, C. (2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

Η Ευρωπαϊκή Επιτροπή και η κυβέρνηση των ΗΠΑ έχουν αρχίσει τις διαπραγματεύσεις για τη διάδοχο συμφωνία της «Ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ», προκειμένου να τεθεί το νέο σημείο αναφοράς των διατλαντικών ροών[737]. Αναλυτικότερα, στις 25 Μαρτίου 2021, αποτυπώθηκε σε δελτίο τύπου[738] η πρόθεση εντατικοποίησης των διαπραγματεύσεων για την υιοθέτηση ενός νέου πλαισίου διατλαντικών μεταφορών των δεδομένων.

9.3 Κριτικές σκέψεις στη διαμόρφωση του νέου πλαισίου διασυνοριακής ροής δεδομένων από την ΕΕ στις ΗΠΑ

Αναμφισβήτητα, το ΔΕΕ έχει διαδραματίσει καθοριστικής σημασίας ρόλο στη διαμόρφωση των διατλαντικών ροών των προσωπικών δεδομένων. Πιο συγκεκριμένα, το ΔΕΕ έχει ακυρώσει έως σήμερα δύο συμφωνίες μεταξύ ΕΕ και ΗΠΑ, τις «Αρχές του ασφαλούς λιμένα» με την απόφαση Schrems I και την «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» με την απόφαση Schrems II.

Θα πρέπει να σημειωθεί ότι η πρώτη συμφωνία των «Αρχών του ασφαλούς λιμένα», η οποία συνήφθη μεταξύ ΕΕ και ΗΠΑ το 2000, παρέμεινε σε ισχύ για 15 έτη μέχρι την ακύρωσή της το 2015. Η επόμενη συμφωνία της «Ασπίδας προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» παρέμεινε σε ισχύ για 4 έτη, από το 2016 έως το 2020.

Θα μπορούσε να υποστηριχθεί ότι η θέση σε εφαρμογή του GDPR το 2018 αποτέλεσε ένα παράγοντα επηρεασμού του διατλαντικού τοπίου των διασυνοριακών διαβιβάσεων των προσωπικών δεδομένων.

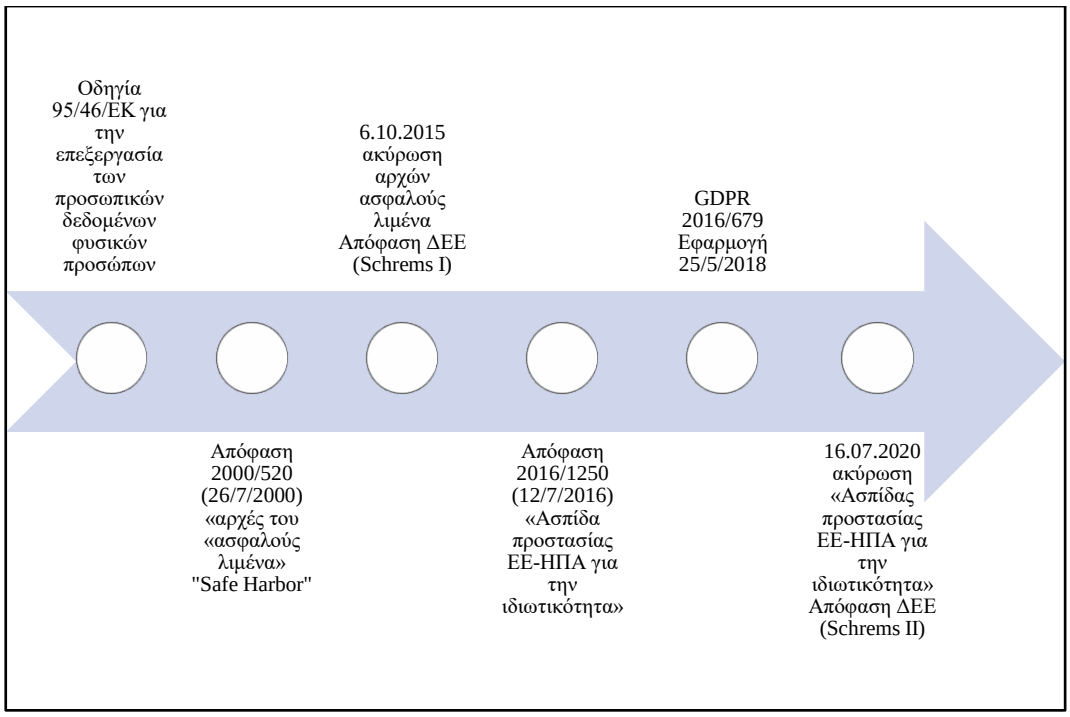
Καθώς η οικονομική σημασία των διατλαντικών ροών των δεδομένων είναι αδιαμφισβήτητη, έχει ανακοινωθεί[739] η πρόθεση υιοθέτησης μίας «πιο ενισχυμένης» ασπίδας, καθιστώντας σαφές ότι ο ρυθμιστής του πλαισίου των διασυνοριακών ροών μεταξύ ΕΕ και ΗΠΑ θα είναι μία αντίστοιχη συμφωνία με τις προϊσχύουσες, υπό νέους όρους, στην οποία θα μπορούν να βασίζονται οι εξαγωγείς των δεδομένων.

---

[737] Βλ. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

[738] European Commission. (2021). Intensifying Negotiations on transatlantic Data Privacy Flow. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443

[739] European Commission. (2021). Intensifying Negotiations on transatlantic Data Privacy Flow. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443



Εικόνα 8. Η πορεία της διατλαντικής ροής δεδομένων μεταξύ ΕΕ-ΗΠΑ

Υπό αυτό το πρίσμα, και με τη διαπίστωση της μη εξασφάλισης ισοδύναμης προστασίας των δεδομένων από την αμερικάνικη νομοθεσία στην απόφαση Schrems II, δύναται να αναζητηθούν ενδεχόμενες διασφαλίσεις στις διατλαντικές διαβιβάσεις δεδομένων. Ειδικότερα, η εξασφάλιση τυποποιημένων και σταθερών εγγυήσεων, με την παράλληλη εξειδίκευση ορισμένων κύριων περιπτώσεων των διαβιβάσεων, θα μπορούσε να τελεσφορήσει στη δημιουργία ενός οριοθετημένου και αναλυτικού πεδίου, το οποίο να διέπει τις διαβιβάσεις των προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ.

ΚΕΦΑΛΑΙΟ 10. Η ΝΟΜΙΚΗ ΡΥΘΜΙΣΗ ΤΗΣ ΔΙΑΣΥΝΟΡΙΑΚΗΣ ΡΟΗΣ ΔΕΔΟΜΕΝΩΝ ΑΠΟ ΤΗΝ ΕΕ ΣΤΟ ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ ΜΕΤΑ ΤΟ BREXIT

10.1 Εισαγωγικές παρατηρήσεις

Στο παρόν κεφάλαιο επιχειρείται η αποσαφήνιση του πλαισίου που διέπει τις μεταφορές προσωπικών δεδομένων από τον ΕΟΧ στο Ηνωμένο Βασίλειο, μετά την ολοκλήρωση του Brexit[740] στις 31 Ιανουαρίου 2020. Η ανάλυση της νομικής ρύθμισης και της σταδιακής αποκρυστάλλωσης του πεδίου των διασυνοριακών ροών, μεταξύ ΕΟΧ και Ηνωμένου Βασιλείου, είναι αξιοσημείωτη, καθώς μετά το Brexit το Ηνωμένο Βασίλειο κατέστη τρίτη χώρα, σύμφωνα με τη νομοθεσία της ΕΕ[741].

10.2 Η μεταβατική ρύθμιση της συμφωνίας Εμπορίου και Συνεργασίας της 31.12.2020

Το Ηνωμένο Βασίλειο αποχώρησε από την ΕΕ στις 31 Ιανουαρίου 2020[742]. Η Συμφωνία Αποχώρησης[743] του Ηνωμένου Βασιλείου από την ΕΕ προέβλεπε μία μεταβατική περίοδο κατά την οποία συνέχισε να ισχύει το δίκαιο της ΕΕ στο Ηνωμένο Βασίλειο, η οποία ίσχυε μέχρι τις 31 Δεκεμβρίου 2020. Στις 31 Δεκεμβρίου 2020 συνήφθη η Συμφωνία Εμπορίου και Συνεργασίας[744] μεταξύ της ΕΕ και του Ηνωμένου Βασιλείου.

Από την 1η Ιανουαρίου 2021 οι διαβιβάσεις προσωπικών δεδομένων από τον ΕΟΧ στο Ηνωμένο Βασίλειο παρέμειναν ελεύθερες, καθεστώς που

[740] Ο όρος αναφέρεται στην αποχώρηση του Ηνωμένου Βασιλείου από την Ευρωπαϊκή Ένωση, Βλ. https://www.oxfordlearnersdictionaries.com/definition/english/brexit

[741] Patel, O., & Lea, N. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. *Available at SSRN 3618937*.

[742] Βλ. https://www.consilium.europa.eu/el/policies/eu-uk-after-referendum/

[743] Συμφωνία για την αποχώρηση του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας από την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα Ατομικής Ενέργειας. 2019/C 384 I/01. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv%3AOJ.CI.2019.384.01.0001.01.ELL&toc=OJ%3AC%3A2019%3A384I%3ATOC

[744] Συμφωνία Εμπορίου και Συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, αφενός, και του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας, Αφετέρου. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:22020A1231(01)

συνεχίστηκε, ως επί το πλείστον, και με την έκδοση της απόφασης επάρκειας[745] του Ηνωμένου Βασιλείου από την Ευρωπαϊκή Επιτροπή στις 28.6.2021. Πιο συγκεκριμένα, για το χρονικό διάστημα των 6 αυτών μηνών (από 01/01/2021 έως 28/06/2021) οι διαβιβάσεις προσωπικών δεδομένων στο Ηνωμένο Βασίλειο διέπονταν από τη Συμφωνία Εμπορίου και Συνεργασίας, η οποία θέσπισε ένα μεταβατικό καθεστώς στο άρθρο FINPROV.10A «Προσωρινή διάταξη για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα στο Ηνωμένο Βασίλειο»[746]. Αναλυτικότερα, στην παρ. 1 του άρθρου FINPROV.10A προβλέπεται ότι για το διάστημα, στο οποίο αναφέρεται η συμφωνία, η διαβίβαση δεδομένων από τον ΕΟΧ στο Ηνωμένο Βασίλειο «δεν θεωρείται διαβίβαση σε τρίτη χώρα».

Παράλληλα, ως προς το διάστημα ισχύος της εν λόγω διάταξης της Συμφωνίας Εμπορίου και Συνεργασίας, αξίζει να γίνει αναφορά στην παρ. 4. Ειδικότερα, στην παρ. 4 προβλέπεται ότι η ελευθερία των διαβιβάσεων των προσωπικών δεδομένων στο Ηνωμένο Βασίλειο θα ισχύει έως 6 μήνες ή έως ότου εκδοθεί απόφαση επάρκειας από την Ευρωπαϊκή Επιτροπή. Η διάταξη αυτή καταδεικνύει την πρόθεση αφενός υιοθέτησης του μοντέλου της απόφασης επάρκειας για τη σχέση των διασυνοριακών διαβιβάσεων Ηνωμένου Βασιλείου και ΕΕ και αφετέρου της άμεσης εξασφάλισής της. Η πρόβλεψη της διάταξης της συμφωνίας για τις διασυνοριακές διαβιβάσεις θα μπορούσε να υποστηριχθεί ότι αναδεικνύει τη σημασία των διεθνών διαβιβάσεων.

Άλλωστε, η άμεση κινητοποίηση για την πραγμάτωση της απόφασης επάρκειας καταδεικνύεται από το δελτίο τύπου[747] της Ευρωπαϊκής Επιτροπής της 19ης Φεβρουαρίου 2021. Η Ευρωπαϊκή Επιτροπή ξεκίνησε στις 19 Φεβρουαρίου 2021 τις διαδικασίες για την υιοθέτηση των αποφάσεων επάρκειας, σχετικά με τις διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα προς το Ηνωμένο Βασίλειο, και πιο συγκεκριμένα μίας απόφασης βάσει του GDPR και μίας απόφασης βάσει της Οδηγίας (ΕΕ) 2016/680[748].

---

[745] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf

[746] Βλ. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_el

[747] Ευρωπαϊκή Επιτροπή. (2021). «Προστασία δεδομένων: σχέδιο απόφασης επάρκειας του Ηνωμένου Βασιλείου». Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/ip_21_661

[748] Ευρωπαϊκή Επιτροπή. (2021). «Προστασία δεδομένων: σχέδιο απόφασης επάρκειας του Ηνωμένου Βασιλείου». Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/ip_21_661

10.3 Η διαμόρφωση του νέου πλαισίου διασυνοριακής ροής δεδομένων από την ΕΕ στο Ηνωμένο Βασίλειο

Στις 28 Ιουνίου 2021, η Ευρωπαϊκή Επιτροπή εξέδωσε δύο αποφάσεις επάρκειας αναφορικά με τη διαβίβαση των προσωπικών δεδομένων προς το Ηνωμένο Βασίλειο (η μία απόφαση επάρκειας[749] σύμφωνα με τον GDPR και η δεύτερη απόφαση επάρκειας[750] σύμφωνα με την Οδηγία (ΕΕ) 2016/680[751]). Και οι δύο αποφάσεις θα ισχύουν έως τις 27 Ιουνίου 2025[752]. Θα πρέπει να σημειωθεί ότι η απόφαση επάρκειας για το Ηνωμένο Βασίλειο κατέστη η δεύτερη απόφαση της Ευρωπαϊκής Επιτροπής που εδράζεται στον GDPR, μετά την έκδοση της απόφασης επάρκειας για την Ιαπωνία.

Αξίζει να τονιστεί ότι τα προσωπικά δεδομένα τα οποία διαβιβάζονται από την ΕΕ στο Ηνωμένο Βασίλειο για τους σκοπούς ελέγχου της μετανάστευσης στο Ηνωμένο Βασίλειο διαφεύγουν της εμβέλειας της απόφασης επάρκειας[753].

Η νομοθετική προστασία των προσωπικών δεδομένων στο Ηνωμένο Βασίλειο ερείδεται στον «GDPR του Ηνωμένου Βασιλείου»[754] και στον νόμο του 2018 για την προστασία των δεδομένων, οι οποίοι αντικατοπτρίζουν τον GDPR και την Οδηγία (ΕΕ) 2016/680[755].

---

[749] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf

[750] Commission Implementing Decision Of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf

[751] Βλ. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_el

[752] Information Commissioner's Office. Data Protection and the EU. Διαθέσιμο στο: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu

[753] Information Commissioner's Office. Data Protection and the EU. Διαθέσιμο στο: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/

[754] Βλ.https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685632/2018-03-05_Keeling_Schedule.pdf

[755] Ευρωπαϊκή Επιτροπή. (2021). «Προστασία δεδομένων: σχέδιο απόφασης επάρκειας του Ηνωμένου Βασιλείου». Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/ip_21_661

Ειδικότερα, όσον αφορά τον «GDPR του Ηνωμένου Βασιλείου», επιβάλλεται να αναφερθεί ότι αποτελεί κατ' ουσία τη μεταφορά του GDPR στην εθνική νομοθεσία της χώρας, μετά την τροποποίηση κάποιων όρων τεχνικού χαρακτήρα. Παράλληλα, ο νόμος για την προστασία δεδομένων του 2018 (Data Protection Act 2018)[756], ο οποίος ήταν ο εθνικός εφαρμοστικός νόμος της χώρας μετά την έκδοση του GDPR[757], παραμένει σε ισχύ[758].

Επί του παρόντος, τα κράτη, τα οποία έχουν λάβει απόφαση επάρκειας για το επίπεδο προστασίας των δεδομένων τους από την Ευρωπαϊκή Επιτροπή, μπορούν να διαβιβάζουν δεδομένα στο Ηνωμένο Βασίλειο[759]. Παράλληλα, θα πρέπει να αναφερθεί ότι, σύμφωνα με Γραφείο του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου, όλα τα κράτη του ΕΟΧ, το Γιβραλτάρ και τα κράτη που είχαν λάβει απόφαση επάρκειας από την Ευρωπαϊκή Επιτροπή (σε ισχύ στις 31 Δεκεμβρίου 2020), διαθέτουν επάρκεια ως προς την προστασία των δεδομένων για το Ηνωμένο Βασίλειο[760]. Το Ηνωμένο Βασίλειο, όπως αναφέρεται από το Γραφείο του Επιτρόπου Πληροφοριών, διαθέτει την εξουσία να εκδίδει αυτόνομες αποφάσεις επάρκειας[761], οι οποίες αναφέρονται ως κανονισμοί επάρκειας στο άρθρο 17Α του Data Protection Act 2018.

[756]Data Protection Act 2018. Διαθέσιμο στο: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[757] Βλ. https://www.gov.uk/data-protection

[758] Piper, D. L. A. (2021). *Data protection laws of the world: full handbook: United Kingdom.* DLA Piper.

[759]Βλ. https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/

[760] Piper, D. L. A. (2021). *Data protection laws of the world: full handbook: United Kingdom.* DLA Piper.

[761] Information Commissioner's Office. International transfers after the UK exit from the EU Implementation Period. Διαθέσιμο στο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

ΣΥΜΠΕΡΑΣΜΑΤΑ-ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΤΟ ΣΥΓΧΡΟΝΟ ΠΑΓΚΟΣΜΙΟ ΠΛΑΙΣΙΟ ΤΩΝ ΔΙΑΣΥΝΟΡΙΑΚΩΝ ΡΟΩΝ ΤΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Στην παρούσα διατριβή επιχειρήθηκε η ανάδειξη του πεδίου των διασυνοριακών ροών των οικονομικών δεδομένων σε ένα ευρύ φάσμα. Καθώς τα οικονομικά προσωπικά δεδομένα συνιστούν ένα αναπόσπαστο μέρος του σύγχρονου κοινωνικό-οικονομικού γίγνεσθαι, με αξιοσημείωτη οικονομική σημασία[762], κρίθηκε σκόπιμη η ανάλυσή τους υπό το πρίσμα των κύριων τομέων που τα διέπουν. Πιο συγκεκριμένα, αφενός παρουσιάστηκαν οι ρυθμίσεις των μεταφορών των προσωπικών δεδομένων σε διεθνές και ευρωπαϊκό επίπεδο, και αφετέρου αναδείχθηκε η θέαση των κύριων ζητημάτων ιδιωτικότητας μέσα από επιλεγμένες σύγχρονες τεχνολογικές εξελίξεις, υπό το πρίσμα του ευρωπαϊκού ισχύοντος δικαίου των προσωπικών δεδομένων και ειδικότερα τον GDPR.

Αναλυτικότερα, η μελέτη του περιβάλλοντος της διασυνοριακής ροής των οικονομικών δεδομένων, η οποία συμπεριέλαβε τα φορολογικά δεδομένα, τα χρηματοοικονομικά δεδομένα και τη διασυνοριακή ροή των δεδομένων στο διεθνές εμπόριο, κατέδειξε το μέγεθος της ποικιλότητας του πεδίου. Η ανάλυση του πλαισίου της διασυνοριακής ροής των δεδομένων και η θέση της ιδιωτικότητας μέσα σε αυτό, δύναται να υποστηριχθεί ότι αναδεικνύει τη δυνατότητα υιοθέτησης της διάκρισης των διαβιβάσεων των προσωπικών δεδομένων. Η κατηγοριοποίηση, ως εκ τούτου, των διαβιβάσεων των προσωπικών δεδομένων θα μπορούσε να συμβάλει στη δημιουργία τυποποιημένων σχημάτων, εισαγόμενων μέσα από κατευθυντήριες γραμμές.

Η ραγδαία ανάπτυξη των νέων τεχνολογιών στον τομέα της Πληροφορικής θέτει συνεχώς νέα πεδία ανταλλαγής δεδομένων, στα οποία καθίσταται απαραίτητη η διεθνής μεταφορά των προσωπικών δεδομένων. Στην παρούσα μελέτη, η παρουσίαση των ζητημάτων ιδιωτικότητας των παγκόσμιων δικτύων 5ης γενιάς, καθώς και η παρουσίαση των ζητημάτων ιδιωτικότητας των αναδυόμενων δικτύων 6ης γενιάς κατέδειξαν την ανάγκη επαγρύπνησης και εξειδικευμένης προστασίας των προσωπικών δεδομένων στο πλαίσιο εφαρμογής των νέων τεχνολογιών. Επιπλέον, το πλαίσιο διαφύλαξης των προσωπικών δεδομένων των παιδιών στο Διαδίκτυο των Πραγμάτων, και ειδικότερα μέσα στο περιβάλλον των έξυπνων σπιτιών, αναλύθηκε με στόχο την προστασία μίας ευαίσθητης μερίδας ατόμων απέναντι σε μία σύγχρονη και παγκόσμιας εμβέλειας

[762] Βλ. Nguyen, D., & Paczos, M. (2020). Measuring the economic value of data and cross-border data flows: A business perspective. Διαθέσιμο στο: https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en

τεχνολογία, η οποία διεισδύει ολοένα περισσότερο στην κοινωνικοοικονομική πραγματικότητα. Μέσα από την αποσαφήνιση καίριων τεχνολογιών στο παρόν πόνημα αναδεικνύεται, εξίσου με τα διαφορετικά περιβάλλοντα διακίνησης των οικονομικών προσωπικών δεδομένων, η συμβολή της κατηγοριοποίησης των διαβιβάσεων με κριτήριο την εκάστοτε εμπλεκόμενη τεχνολογία της επιστήμης της Πληροφορικής.

Επιπρόσθετα, τα ζητήματα ιδιωτικότητας που εγείρουν οι νέες τεχνολογίες, πέραν της ανάγκης εξειδικευμένης αντιμετώπισης, καταδεικνύουν τη σημασία της εκ των προτέρων εξέτασής τους. Αναλυτικότερα, η παρούσα μελέτη εστίασε στην εκπλήρωση των όρων που θέτει η προστασία των προσωπικών δεδομένων, σε σχέση με τις επιλεγμένες καινοτομίες, καλύπτοντας ένα νέο πεδίο, καθότι η εστίαση στον τομέα της έρευνας επικεντρώνεται στην ασφάλεια των δεδομένων. Η ασφάλεια των προσωπικών δεδομένων αποτελεί αναπόσπαστο μέρος της προστασίας των διασυνοριακών ροών των δεδομένων, και εν γένει όλων των επεξεργασιών, χωρίς ωστόσο να αποτελεί το μόνο. Ορισμένες προτάσεις στην κατεύθυνση αυτή δύνανται να περιλαμβάνουν: τη διεύρυνση του καταλόγου με τις πράξεις που απαιτούν εκτίμηση αντίκτυπου με την εισχώρηση καινοτόμων τεχνολογιών που θα εξειδικεύονται όσο το δυνατόν περισσότερο, τον σχεδιασμό πρωτοκόλλων ασφαλείας με γνώμονα τα ζητήματα ιδιωτικότητας και τα δικαιώματα των υποκειμένων των δεδομένων και εν γένει την εγγύτερη συνεργασία της επιστήμης της Πληροφορικής με τη Νομική επιστήμη στο στάδιο σχεδιασμού και εφαρμογής των νέων τεχνολογιών.

Η παρουσίαση των διεθνών νομικών ρυθμίσεων για τη διασυνοριακή ροή των οικονομικών δεδομένων με χρονολογική ταξινόμηση, στο παρόν πόνημα, επιχείρησε να προβάλλει την αυτοτελή ρύθμιση των διεθνών διαβιβάσεων, τη σημασία που τους αποδίδεται καθώς και τη διαχρονική εξέλιξη του πεδίου. Η εν λόγω ανάλυση στοχεύει στη βέλτιστη κατανόηση του διεθνούς πλαισίου των διασυνοριακών ροών των δεδομένων και στην αλληλεπίδρασή τους με τις εθνικές και ευρωπαϊκές ρυθμίσεις. Σε εθνικό επίπεδο, από τις νομοθεσίες των διαφορετικών χωρών όλων των ηπείρων, οι οποίες συμπεριλήφθησαν στην παρούσα μελέτη, συνάγεται η ετερογένεια αφενός των ρυθμίσεων για τη διασυνοριακή ροή των προσωπικών δεδομένων και αφετέρου του χρονικού σημείου θέσπισης των νομοθεσιών για την προστασία των προσωπικών δεδομένων. Λαμβάνοντας υπόψη τα εν λόγω στοιχεία, η έλλειψη ομοιογένειας στους μηχανισμούς διασυνοριακής ροής των δεδομένων μπορεί να υποστηριχθεί ότι δύναται να επηρεάσει τους πρακτικούς μηχανισμούς επιβολής. Συνάγεται, επομένως, το συμπέρασμα ότι οι υπεύθυνοι της επεξεργασίας των δεδομένων διαφορετικών κρατών, ενώ δρουν σε ένα παγκοσμιοποιημένο οικονομικό

περιβάλλον, έρχονται αντιμέτωποι με διαφορετικά ζητήματα που εγείρουν οι εθνικές νομοθεσίες. Περαιτέρω, θα πρέπει να αναφερθεί ότι ένα μέρος των εθνικών νομοθεσιών αναφέρει τις έννοιες του «ισοδύναμου», «αντίστοιχου» κ.ο.κ. επιπέδου προστασίας των δεδομένων τρίτων χωρών ως βάση για τις διεθνείς διαβιβάσεις. Ως εκ τούτου, αρωγός στην προστασία των προσωπικών δεδομένων, σε παγκόσμιο επίπεδο, όταν διαβιβάζονται σε έδαφος τρίτων χωρών θα μπορούσε να αποτελέσει η υιοθέτηση σύγχρονων βασικών κανόνων για την προστασία των προσωπικών δεδομένων εν γένει, με παγκόσμια εμβέλεια. Παράλληλα, η υλοποίηση ενός διεθνούς αποθετηρίου, το οποίο να περιλαμβάνει τους εκάστοτε ισχύοντες εθνικούς νόμους για την προστασία των προσωπικών δεδομένων των κρατών στην αγγλική γλώσσα, θα μπορούσε να συμβάλει στην καλύτερη αξιολόγηση του επιπέδου προστασίας των τρίτων χωρών.

Σε ευρωπαϊκό επίπεδο, η εκτενής και με χρονολογική σειρά ανάλυση των νομοθετικών ρυθμίσεων της ΕΕ για τα προσωπικά δεδομένα, κατέδειξε την ενισχυμένη ανάγκη ρύθμισης της διασυνοριακής ροής των δεδομένων, ειδικά, και των προσωπικών δεδομένων γενικά, συνοδεύοντας την ολοένα αυξημένη ροή τους[763]. Από τη διαχρονική παρουσίαση των ενωσιακών ρυθμίσεων, στον τομέα προστασίας των προσωπικών δεδομένων, διαφαίνεται μία αυξητική τάση με πρόθεση περαιτέρω εξειδίκευσης, η οποία διέπει την επιδίωξη της προστασίας τους.

Αναλυτικότερα, ο κεντρικός άξονας του ενωσιακού δικαίου για την προστασία των προσωπικών δεδομένων αποτελείται από τον GDPR, ο οποίος συνιστά σημείο αναφοράς για την παρούσα μελέτη. Η ίδια η νομική φύση του Κανονισμού, αλλά και οι επιδιώξεις ενίσχυσης του πλαισίου προστασίας των δεδομένων, τον έχουν καταστήσει ένα από τα πιο αναλυτικά, σαφή και ως εκ τούτου αυστηρά νομικά πλαίσια σε παγκόσμιο επίπεδο[764]. Ειδικότερα, ως προς τους ευρωπαϊκούς μηχανισμούς διασυνοριακής ροής δεδομένων από τον ΕΟΧ σε τρίτες χώρες, θα πρέπει να αναφερθεί ότι αυτοί αποτυπώθηκαν στον GDPR αναλυτικότερα σε σχέση με την προϊσχύουσα Οδηγία 95/46/ΕΚ.

Παράλληλα, αξιοσημείωτη θα πρέπει να θεωρηθεί η επίδραση της νομολογίας στη διαμόρφωση του εκάστοτε ισχύοντος ευρωπαϊκού πλαισίου για τις διασυνοριακές ροές. Καθώς οι εκδοθείσες αποφάσεις επάρκειας από την Ευρωπαϊκή Επιτροπή παραμένουν σχετικά περιορισμένες, οι διασυνοριακές ροές

[763] Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη, σελ. 119.

[764] Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR interference with next generation 5G and IoT networks. *IEEE Access*, *8*, 108052-108061.

των δεδομένων επαφίενται, ως προς ένα μεγάλο μερίδιο τρίτων χωρών, στα υπόλοιπα εργαλεία διεθνών διαβιβάσεων (άρθρα 46 έως 49 GDPR). Ως προς τα καίρια και σύγχρονα ζητήματα του πεδίου, η αντανάκλαση της απόφασης του ΔΕΕ στην υπόθεση C-311/18 (Schrems II) έχει δημιουργήσει επιπρόσθετες προϋποθέσεις στο εργαλείο διαβίβασης των κατάλληλων εγγυήσεων[765]. Πιο συγκεκριμένα, η αξιολόγηση του επιπέδου προστασίας των τρίτων χωρών για την επιλογή διαβίβασης, βάσει κατάλληλων εγγυήσεων, επισύρει μία διαδικασία εκτίμησης του επιπέδου προστασίας της τρίτης χώρας και την εφαρμογή πρόσθετων μέτρων αν κρίνεται απαραίτητο[766]. Εφόσον, λοιπόν, οι εξαγωγείς των προσωπικών δεδομένων οφείλουν να πραγματοποιούν εκτίμηση της προστασίας των προσωπικών δεδομένων των τρίτων χωρών, με σημείο αναφοράς την εκάστοτε διαβίβαση, θα ήταν ωφέλιμη η συστηματοποίηση της διαδικασίας με την εφαρμογή εκτίμησης των επιπτώσεων της μεταφοράς των δεδομένων (Transfer Impact Assessment). Η εκτίμηση των επιπτώσεων της μεταφοράς των δεδομένων, στα πρότυπα της εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων του άρθρου 35 παρ. 4 του GDPR, θα μπορούσε να συμβάλει στην ενίσχυση της κατηγοριοποίησης και αυτοματοποίησης ορισμένων διαβιβάσεων. Η υιοθέτηση υποστηρικτικών εργαλείων σε αυτήν την κατεύθυνση, όπως εξειδικευμένων λογισμικών, θα μπορούσε να ενισχύσει την αποτελεσματικότητα αυτών των διαδικασιών, μέσω της βελτίωσης της φαρέτρας των εξαγωγέων των προσωπικών δεδομένων. Ωστόσο, θα πρέπει να αναφερθεί ότι ένα λογισμικό εκτίμησης αντίκτυπου της μεταφοράς των προσωπικών δεδομένων, σε ευρωπαϊκό επίπεδο, επιβάλλεται να εμπεριέχει τις νομοθεσίες των τρίτων κρατών που αφορούν τα προσωπικά δεδομένα, αλλά και νομοθεσίες που δύνανται να επηρεάσουν την προστασία των προσωπικών δεδομένων, στην πράξη, άμεσα ή έμμεσα. Ένα τέτοιο εγχείρημα, βέβαια, προϋποθέτει παγκόσμια συνεργασία, η οποία ως έρεισμα λαμβάνει το αναπόσπαστο πεδίο των διεθνών οικονομικών σχέσεων.

Όσον αφορά το πεδίο των διατλαντικών διασυνοριακών ροών μεταξύ ΕΕ και ΗΠΑ, θα μπορούσε να αναφερθεί ότι οι εξελίξεις του επηρεάζουν το πλαίσιο των διασυνοριακών ροών των δεδομένων εν γένει. Ειδικότερα, ένα κύριο σημείο των διαχρονικών εξελίξεων των διαβιβάσεων αποτελεί η έννοια της εθνικής

[765] Βλ. C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

[766] Βλ. Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

ασφάλειας σε σχέση με την προστασία της ιδιωτικότητας. Η στόχευση στο εν λόγω ζήτημα με την προσπάθεια εξεύρεσης των κατάλληλων σταθμίσεων, ανάμεσα σε δύο διαφορετικά νομικά συστήματα, θα μπορούσε να συμβάλει στην εξεύρεση ενός αποτελεσματικού και βιώσιμου πλαισίου.

Η παρούσα διατριβή συμβάλλει στην αποκρυστάλλωση του σύγχρονου πλαισίου των διασυνοριακών ροών των οικονομικών δεδομένων, λαμβάνοντας υπόψη ένα ευρύ φάσμα νομοθεσιών, με σημείο αναφοράς το ευρωπαϊκό πλαίσιο. Ειδικότερα, το πόνημα συνεισφέρει στην οριοθέτηση της έννοιας των διασυνοριακών ροών των δεδομένων και συγκεκριμένα των οικονομικών, στη συσχέτιση σύγχρονων τεχνολογικών επιτευγμάτων του τομέα της Πληροφορικής Επιστήμης με τον ευρύτερο τομέα της προστασίας της ιδιωτικότητας και την αποσαφήνιση του διεθνούς και ευρωπαϊκού νομικού πλαισίου επί του θέματος. Επί του παρόντος υφίστανται πολλές πλευρές του πεδίου των διασυνοριακών ροών των οικονομικών δεδομένων που δύνανται να διερευνηθούν. Ο τομέας των διασυνοριακών ροών των οικονομικών δεδομένων, και ειδικότερα η νομική του προσέγγιση, θα συνεχίσει τα επόμενα έτη να αναδεικνύει ζητήματα, ενόψει των αναδυόμενων τεχνολογιών στον τομέα της Πληροφορικής αλλά και τον συγκερασμό τους με τα νέα δεδομένα του οικονομικού τομέα, όπως η εισχώρηση των ψηφιακών νομισμάτων. Η μελέτη της διασυνοριακής ροής των οικονομικών δεδομένων επιδιώκει, πέραν της θεσμικής ετοιμότητας ως προς το πεδίο, την επαγρύπνηση όλων των τομέων του σύγχρονου κοινωνικοοικονομικού γίγνεσθαι ως προς την προστασία των προσωπικών δεδομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΑΡΘΡΟΓΡΑΦΙΑ

I. ΕΛΛΗΝΟΓΛΩΣΣΗ

1.Jougleux, P. (2016). *Ευρωπαϊκό Δίκαιο του Διαδικτύου*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

2.Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2007). Η πλοήγηση των ανηλίκων στο Διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων. *Αρμενόπουλος, 6,* 848-854.

3.Αλεξανδροπούλου - Αιγυπτιάδου, Ε. (2007). Προσωπικά δεδομένα (Νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους). Εκδ. Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή.

4.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2004). Ηλεκτρονική επεξεργασία δεδομένων οικονομικής συμπεριφοράς από την «Τειρεσίας Α.Ε.» (θεσμικό πλαίσιο). *Δελτίο Ένωσης Ελληνικών Τραπεζών, Β' τριμ.,* 25-32.

5.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2004). Ηλεκτρονική επεξεργασία προσωπικών δεδομένων στο πεδίο της τραπεζικής δραστηριότητας (Νομικό Πλαίσιο). *Αρμενόπουλος 10,* 1377-1395.

6.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). Διασυνοριακή ροή προσωπικών δεδομένων από την ΕΕ στις ΗΠΑ: Η πρόσφατη απόφαση του ΔΕΕ ενόψει της σχετικής δραστηριότητας του Facebook (C-362/2014, M. Schrems κατά Ιρλανδού Επιτρόπου Προστασίας Προσωπικών Δεδομένων). *ΔΙΜΕΕ, 1*, 12-24.

7.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2016). *Προσωπικά Δεδομένα.* Νομική Βιβλιοθήκη.

8.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2018). Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679. *ΔΙΜΕΕ, 1*, 5-19.

9.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Διασυνοριακή ροή δεδομένων υγείας, Πρακτικά 5ου Συνεδρίου ιατρικής ευθύνης και βιοηθικής – Δεδομένα υγείας και γενετικά δεδομένα, Αθήνα 19 Ιανουαρίου 2018, εκδ. Παπαζήση.

10.Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2019). Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679/ΕΕ - Προκλήσεις εφαρμογής, Πρακτικά 1ου διεπιστημονικού συνεδρίου «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής, Νομική Σχολή ΔΠΘ, Κομοτηνή 25-26 Μαΐου 2018, εκδ. Νομική Βιβλιοθήκη, Αθήνα.

11. Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2021). Σταθμίσεις συμφερόντων και νομοθετικές επιλογές στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). *ΔΙΤΕ, 3*, 367-376.

12. Αλεξανδροπούλου-Αιγυπτιάδου, Ε., Μαυρίδης, Ι. (2007). Η προστασία των προσωπικών δεδομένων ενόψει της εφαρμογής της νέας τεχνολογίας της ταυτοποίησης με ραδιοσυχνότητες (R.F.I.D.) – Νομική και τεχνολογική προσέγγιση. *Αρμενόπουλος, 4*, 493-504.

13. Αναστασόπουλος, Δ. (2016). *Φορολογικά δεδομένα και προστασία φορολογικού απορρήτου* σε *Ένωση Ελλήνων Νομικών e-ΘΕΜΙΣ, Επίκαιρα Ζητήματα Φορολογικού Δικαίου.* Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη, 285-301.

14. ΑΠΔΠΧ. (2007). Ετήσια έκθεση 2006. Εθνικό τυπογραφείο, Αθήνα. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-12/DPA_ANNUAL_REPORT_2006.PDF

15. ΑΠΔΠΧ. Συμφωνία μεταξύ ΕΕ και ΗΠΑ σχετικά με τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων. Διαθέσιμο στο: https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/megales_baseisdedomenon/TFTP

16. Απόφαση 2006/729/ΚΕΠΠΑ/ΔΕΥ του Συμβουλίου, της 16ης Οκτωβρίου 2006, για την υπογραφή, εξ ονόματος της Ευρωπαϊκής Ένωσης, συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής για την επεξεργασία και τη διαβίβαση δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) από τους αερομεταφορείς στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32006D0729

17. Απόφαση 2007/533/ΔΕΥ του Συμβουλίου, της 12ης Ιουνίου 2007, σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:02007D0533-20070827&from=FR

18. Απόφαση 2007/551/ΚΕΠΠΑ/ΔΕΥ του Συμβουλίου της 23ης Ιουλίου 2007 για την υπογραφή, εξ ονόματος της Ευρωπαϊκής Ένωσης, συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής για την επεξεργασία και τη διαβίβαση δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) από τους αερομεταφορείς στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών (DHS) (Συμφωνία 2007 PNR). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32007D0551

19. Απόφαση της Επιτροπής (2000/518/ΕΚ), της 26ης Ιουλίου 2000, δυνάμει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα που παρέχεται στην Ελβετία. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32000D0518

20. Απόφαση της Επιτροπής (2000/520/ΕΚ), της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32000D0520

21. Απόφαση της Επιτροπής (2002/2/ΕΚ), της 20ής Δεκεμβρίου 2001, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα του καναδικού νόμου περί προστασίας των δεδομένων προσωπικού χαρακτήρα και ηλεκτρονικών εγγράφων.

22. Απόφαση της Επιτροπής (2003/490/ΕΚ), της 30ής Ιουνίου 2003, δυνάμει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια προστασίας δεδομένων προσωπικού χαρακτήρα στην Αργεντινή.

23. Απόφαση της Επιτροπής (2004/535/ΕΚ), της 14ης Μαΐου 2004, σχετικά με την ικανοποιητική προστασία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στο φάκελο των επιβατών (Passenger Name Record) αεροπορικών μεταφορών ο οποίος διαβιβάζεται στο Bureau of Customs and Border Protection (υπηρεσία τελωνείων και προστασίας των συνόρων) των Ηνωμένων Πολιτειών της Αμερικής [κοινοποιηθείσα υπό τον αριθμό Ε(2004) 1914]. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32004D0535

24.Απόφαση της Επιτροπής (2011/61/ΕΕ), της 31ης Ιανουαρίου 2011, σχετικά με την επάρκεια, σύμφωνα με την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της προστασίας των δεδομένων προσωπικού χαρακτήρα από το Κράτος του Ισραήλ όσον αφορά την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32011D0061

25.Απόφαση του Συμβουλίου (2004/496/ΕΚ), της 17ης Μαΐου 2004, για τη σύναψη συμφωνίας μεταξύ της Ευρωπαϊκής Κοινότητας και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση των καταστάσεων με τα ονόματα των επιβατών από τους αερομεταφορείς προς το Υπουργείο Εσωτερικής Ασφάλειας, Υπηρεσία Τελωνείων και Προστασίας των Συνόρων των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32004D0496

26.Απόφαση του Συμβουλίου (2013/157/ΕΕ), της 7ης Μαρτίου 2013, που ορίζει την ημερομηνία εφαρμογής της απόφασης 2007/533/ΔΕΥ σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II). Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32013D0157

27.Αρμαμέντος, Π., Σωτηρόπουλος, Β. (2005). *Προσωπικά δεδομένα - Ερμηνεία Ν. 2472/1997*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

28.Βασιλάκη, Β. (2020). *Συντηρητική κατάσχεση στα χέρια τρίτου*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

29.Βλαχόπουλος, Σ. (2018). Διασυνοριακή μεταβίβαση δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση προς τρίτες χώρες: Οι τελευταίες εξελίξεις, Πρακτικά Ημερίδας «Προστασία των δεδομένων προσωπικού χαρακτήρα», Κέντρο Διεθνούς και Ευρωπαϊκού Οικονομικού Δικαίου, 18 Σεπτεμβρίου 2017, Επιμέλεια: Τζώρτζη, Β., εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

30.Γιαννόπουλος, Γ. (2001). Προστασία προσωπικών δεδομένων και διασυνοριακή ροή πληροφοριών. Το πρόβλημα του «ικανοποιητικού επιπέδου προστασίας». *ΔτΑ*, 5, 733 κ. επ.

31.Γνωμοδότηση του Ευρωπαίου Επόπτη Προστασίας Δεδομένων επί της πρότασης απόφασης του Συμβουλίου σχετικά με τη σύναψη της

συμφωνίας μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης για τη χρήση και τη διαβίβαση των φακέλων επιβατών (φάκελοι PNR) στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών (2012/C 35/03). Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/publication/11-12-09_us_pnr_el.pdf

32.Δετσαρίδης, Χ. (2012). Φορολογικό απόρρητο και δημοσιοποίηση φορολογικών στοιχείων οφειλετών του Δημοσίου υπό το πρίσμα του εθνικού και ενωσιακού νομοθέτη. *Εφημερίδα Διοικητικού Δικαίου, 4,* 450-458.

*33.*Δούβλης, Β. (2015). Διεθνείς δράσεις κατά της φοροδιαφυγής-φοροαποφυγής: «Η Μεγάλη Χίμαιρα»; *ΔΕΕ, 8-9,* 769-787.

34.Δούβλης, Β. (2019). Η Υποχρεωτική Αυτόματη Ανταλλαγή Φορολογικών Πληροφοριών και η επέκτασή της στις Διασυνοριακές Ρυθμίσεις με την Οδηγία 2018/822/ΕΕ. *ΔΕΕ, 1,*1-13.

35.Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την από κοινού επανεξέταση της εφαρμογής της συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής για τους σκοπούς του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας, COM/2017/031 final, Διαθέσιμο στο: http://ec.europa.eu/transparency/regdoc/rep/1/2013/EL/1-2013-842-EL-F1-1.Pdf

36.Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016D1250

37.Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής της 4ης Ιουνίου 2021 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32021D0914

38.Ενοποιημένη απόδοση της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης *ΕΕ C 326 της 26.10.2012.* Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:12012E/TXT

39.Ευρωπαϊκή Επιτροπή. (2021). «Προστασία δεδομένων: σχέδιο απόφασης επάρκειας του Ηνωμένου Βασιλείου». Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/el/ip_21_661

40.Ευρωπαϊκό Κοινοβούλιο. Ψήφισμα 2013/2831 σχετικά με την αναστολή της συμφωνίας TFTP ως αποτέλεσμα της παρακολούθησης εκ μέρους της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ.

41.Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 2/2018 αναφορικά με τις παρεκκλίσεις που προβλέπονται στο άρθρο 49 του Κανονισμού 2016/679». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_el

42.Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2018). «Κατευθυντήριες γραμμές 3/2018 σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ (άρθρο 3)». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

43.Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Κατευθυντήριες γραμμές 2/2020 σχετικά με το άρθρο 46 παράγραφος 2 στοιχείο α) και το άρθρο 46 παράγραφος 3 στοιχείο β) του κανονισμού 2016/679 για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και δημόσιων αρχών και φορέων εκτός ΕΟΧ». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_el

44.Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συστάσεις 01/2020 σχετικά με τα μέτρα που συμπληρώνουν τα εργαλεία διαβίβασης για τη διασφάλιση της συμμόρφωσης με το επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα στην ΕΕ». Διαθέσιμο στο:

https://edpb.europa.eu/our-work-tools/documents/publicconsultations/2020/recommendations-012020-measures-supplement_el

45.Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2020). «Συχνές ερωτήσεις σχετικά με την απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης στην υπόθεση C- 311/18 - Επίτροπος προστασίας δεδομένων κατά Facebook Ireland Ltd και Maximillian Schrems». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_el

46.Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. (2021). «Συστάσεις 1/2021 σχετικά με τα σημεία αναφοράς για την επάρκεια βάσει της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου». Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_el

47.Θεοχαροπούλου, Ε. (2016). *Φορολογική διαφάνεια και Ανταλλαγή πληροφοριών σε καιρούς δημοσιονομικής και παγκόσμιας οικονομικής κρίσης*. Αφοί Κυριακίδη εκδόσεις Α.Ε.

48.Θεοχαροπούλου, Ε. (2019). Οι νέες τεχνολογίες στο Φορολογικό Δίκαιο: Ευκαιρία ή απειλή; *ΔΙΜΕΕ, 3*, 300-308.

49.Θεοχαροπούλου, Ε. (2021). *Η άμεση φορολογία της ψηφιακής οικονομίας και η δημιουργία αξίας*. Αφοί Κυριακίδη εκδόσεις Α.Ε.

50.Ιγγλεζάκης, Ι. (2003). ΔΕΚ της 6.11.2003, C-101/01, Gota Hovratt – Bodil Lindqvist. *Επισκόπηση Εμπορικού Δικαίου, 4,* 1041-1051.

51.Ιγγλεζάκης, Ι. (2003). *Ευαίσθητα προσωπικά δεδομένα*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

52.Ιγγλεζάκης, Ι. (2006) *Προστασία προσωπικών δεδομένων στο σύστημα πληροφοριών ΤΕΙΡΕΣΙΑΣ.* Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

53.Ιγγλεζάκης, Ι. (2021). *Δίκαιο Πληροφορικής*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

54.Κανελλοπούλου-Μπότη, Μ. (2009). Η προστασία της ιδιωτικής ζωής και η ευρωπαϊκή νομοθεσία για τα προσωπικά δεδομένα-σκέψεις σε σχέση με την προστασία της ιδιωτικής ζωής στις ΗΠΑ στον *Τιμητικό Τόμο Μιχ. Π. Σταθόπουλου, τόμος ΙΙ*. εκδ. Αντ.Ν. Σάκκουλα. Αθήνα-Κομοτηνή, σελ.809-823. Διαθέσιμο στο: http://bottis.ihrc.gr/en/publications/2009/

55.Κέντρο Ερευνών Δημοσίου Διεθνούς Δικαίου, & Ινστιτούτο Μικρών Επιχειρήσεων της Γενικής Συνομοσπονδίας Επαγγελματιών Βιοτεχνών Εμπόρων Ελλάδας (2016). Ο Παγκόσμιος Οργανισμός Εμπορίου, η GATS και η Ελληνική Αγορά Υπηρεσιών: μία συνοπτική παρουσίαση. Διαθέσιμο στο: https://www.athenspil.law.uoa.gr/fileadmin/depts/law.uoa.gr/athenspil/uploads/gats_memo_tlc.pdf

56.Κόμνιος, Κ. (2020). *Γενικός κανονισμός για την προστασία δεδομένων*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

57.Λωσταράκου, Κ. (2016). *Διακίνηση τραπεζικών δεδομένων και δικαιώματα υποκειμένων* σε Κοτσαλής Λ. (επιμ.) *Προσωπικά δεδομένα (Ανάλυση - Σχόλια - Εφαρμογή)*. Νομική Βιβλιοθήκη.

58.Μεταξάκης, Ε. (2014). Η διακρατική ηλεκτρονική ροή ευαίσθητων προσωπικών δεδομένων – Το ρυάκι που έγινε χείμαρρος. *ΔΙΜΕΕ, 2*, 170-178.

59.Μήτρου, Λ. (2010). Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών.* Αθήνα: Παπασωτηρίου.

60.Μήτρου, Λ. (2012). *Η δημοσιότητα της κύρωσης ή η κύρωση της δημοσιότητας*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

61.Μήτρου, Λ. (2017). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (νέο δίκαιο-νέες υποχρεώσεις-νέα δικαιώματα)*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

62.Μυλώση, Μ. (2015). Η έννομη προστασία των δεδομένων οικονομικής συμπεριφοράς από την αθέμιτη ηλεκτρονική επεξεργασία τους: συγκριτική μελέτη της νομικής ρύθμισης σε Ελλάδα και Γαλλία.

63.Μυλώση, Μ., Αλεξανδροπούλου-Αιγυπτιάδου, Ε. (2015). Προσωπικά δεδομένα οικονομικής συμπεριφοράς και η ηλεκτρονική επεξεργασία τους από την Τειρεσίας Α.Ε. *ΔΙΜΕΕ, 1*, 25-37.

64.Νούλας, Α. Γ. (2005). *Χρήμα και τράπεζες*. Θεσσαλονίκη.

65.Ομάδα εργασίας του άρθρου 29. (2005). «Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995». Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_el.pdf

66.Ομάδα εργασίας του άρθρου 29. (2016). «Κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία». Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/itemType/1360

67.Ομάδα Εργασίας του Άρθρου 29. (2017). «Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679». Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/611236

68.Ομάδα εργασίας του άρθρου 29. (2018). «Σημεία αναφοράς για την επάρκεια». Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-02/wp254%20rev%200.1_EL.pdf

69.Παναγοπούλου-Κουτνατζή, Φ. (2019). Συνταγματικές προεκτάσεις των μηχανισμών διευρύνσεως της προστασίας δεδομένων προσωπικού χαρακτήρα πέραν της ΕΕ: Εξωεδαφική εφαρμογή του ΓΚΠΔ και διασυνοριακή διαβίβαση δεδομένων. *ΔΙΜΕΕ, 4,* 504-520.

70.Παπακωνσταντίνου, Ε. (2010). *Δίκαιο πληροφορικής*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

*71.*Πλιαβέσης, Γ. (2019). *Η προστασία των προσωπικών δεδομένων στη σχέση τράπεζας – πελάτη.* Νομική Βιβλιοθήκη.

72.Πρωτοπαπαδάκης, Ε. Δ. (2016). *Προσωπικά δεδομένα: Μια ηθική προσέγγιση* σε Κοτσαλής Λ. (επιμ.) *Προσωπικά δεδομένα (Ανάλυση - Σχόλια - Εφαρμογή)*. Νομική Βιβλιοθήκη.

73.Ρίζου, Σ. (2019). Διασυνοριακή ροή οικονομικών δεδομένων: Η Συμφωνία SWIFT σε: Αλεξανδροπούλου, Ε., Δαλακούρας, Θ., Μαστροκώστας, Χ. (2019). Πρακτικά 1ου διεπιστημονικού συνεδρίου «Δίκαιο και Πληροφορική»: Αντιμετωπίζοντας τις προκλήσεις της ψηφιακής εποχής. Νομική Σχολή ΔΠΘ. Κομοτηνή 25-26 Μαΐου 2018. εκδ. Νομική Βιβλιοθήκη, Αθήνα.

74.Σαατζίδου-Παντελιάδου, Ε. (2006). Νέοι κανόνες δικαίου στο πλαίσιο της Νέας Οικονομίας: το παράδειγμα της νομικής ρύθμισης της ηλεκτρονικής επεξεργασίας των προσωπικών δεδομένων με έμφαση στην επεξεργασία των δεδομένων οικονομικής συμπεριφοράς.

75.Σαχπεκίδου, Ε. Ρ. (2011). *Ευρωπαϊκό Δίκαιο*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

76.Στεργίου, Α. (2017). *Δίκαιο κοινωνικής ασφάλισης*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

77.Σύμβαση εφαρμογής της συμφωνίας του Σένγκεν της 14ης Ιουνίου 1985 μεταξύ των κυβερνήσεων των κρατών της Οικονομικής Ένωσης Μπενελούξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας, σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A42000A0922%2802%29

78.Συμβούλιο της Ευρώπης. (2018). *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων*. Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης.

79.Συμβούλιο της Ευρώπης. Αιτιολογική Έκθεση της Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, Στρασβούργο, 28.1.1981.

80.Συμβούλιο της Ευρώπης. Αιτιολογική Έκθεση του τροποποιητικού Πρωτοκόλλου της Σύμβασης για την προστασία των ατόμων σε σχέση με την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (223/2018).

81.Συμβούλιο της Ευρώπης. Εκσυγχρονισμένη Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, CETS αριθ. 223, 2018.

82.Συμβούλιο της Ευρώπης. Πρόσθετο Πρωτόκολλο στη Σύμβαση για την προστασία των προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχετικά με τις εποπτικές αρχές και τη διασυνοριακή ροή δεδομένων, CETS αριθ. 181, 2001.

83.Συμβούλιο της Ευρώπης. Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, CETS αριθ. 108, 1981.

84.Συμφωνία για την αποχώρηση του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας από την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα Ατομικής Ενέργειας. 2019/C 384 I/01. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=uriserv%3AOJ.CI.2019.384.01.0001.01.ELL&toc=OJ%3AC%3A2019%3A384I%3ATOC

85.Συμφωνία Εμπορίου και Συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, αφενός, και του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας, Αφετέρου. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:22020A1231(01)

86.Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και της Αυστραλίας για την επεξεργασία και τη διαβίβαση, από τους αερομεταφορείς, δεδομένων από τις καταστάσεις με τα ονόματα των επιβατών (PNR) προς την Υπηρεσία Τελωνείων και Προστασίας των Συνόρων της Αυστραλίας. Διαθέσιμο στο: https://www.dpa.gr/sites/default/files/2020-04/CELEX_22012A0714%2801%29_EL_TXT.pdf

87.Συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής για σκοπούς του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:22010A0727(01)

88.Συμφωνία μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης για τη χρήση και τη διαβίβαση των φακέλων ονομάτων επιβατών στο Υπουργείο Εσωτερικής Ασφάλειας των Ηνωμένων Πολιτειών. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A22012A0811%2801%29

89.Τάσσης, Σ. (2015). ΔΕΕ υπόθ. C-362/2014, απόφ. της 6.10.2015 [Διασυνοριακή ροή δεδομένων] (σημ.). *ΔΙΜΕΕ 3*, 498-512.

90.Τζωρτζάτου, Ο. (2015). *Η προστασία των ευαίσθητων προσωπικών δεδομένων της υγείας στη βιοϊατρική έρευνα*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

91.Φινοκαλιώτης, Κ. (2020). *Φορολογικό δίκαιο*. 6η έκδ. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

92.Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης *ΕΕ C 202 της 7.6.2016.* Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A12016P%2FTXT

93.Χατζηνικολάου-Αγγελίδου, Ρ. (2014). *Ιδιωτικό Ασφαλιστικό Δίκαιο*. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

94.Χρήστου, Β. (2017). Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων. Εκδ. Σάκκουλα: Αθήνα-Θεσσαλονίκη.

95.Χριστοδούλου, Κ. (2020). *Δίκαιο Προσωπικών Δεδομένων*. Εκδ. Νομική Βιβλιοθήκη.

96.Χρυσοχόου, Α. (2009). Προστασία προσωπικών δεδομένων & τραπεζικό απόρρητο.

97.Ψαρογίαννη, Σ. (2010). Η διασυνοριακή ροη πληροφοριών στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας και η προστασία των δεδομένων προσωπικού χαρακτήρα.

98.Ψήφισμα της 6ης Ιουλίου 2006 του Ευρωπαϊκού Κοινοβουλίου σχετικά με την παρακολούθηση των δεδομένων τραπεζικών εντολών με το σύστημα SWIFT από τις μυστικές υπηρεσίες των ΗΠΑ, Διαθέσιμο στο: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0317+0+DOC+XML+V0//EL&language=EL

II. ΞΕΝΟΓΛΩΣΣΗ

1.3GPP, 3GPP TS 22.278: “Service requirements for the Evolved Packet System (EPS).” Διαθέσιμο στο: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=641

2.3GPP, 3GPP TS 23.501: “System architecture for the 5G System (5GS)”. Διαθέσιμο στο: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

3.3GPP, 3GPP TS 33.501: Security architecture and procedures for 5G System. Διαθέσιμο στο: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

4.3GPP, TR 22.891 v.2.0.0. “Feasibility Study on New Services and Markets Technology Enablers”. Διαθέσιμο στο : https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897

5.5G PPP Architecture Working Group: *View on 5G Architecture*. (2019) 3rd edition. Διαθέσιμο στο: https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf

6.Ad hoc Committee on Data Protection (CAHDATA). (2018). “Explanatory Report of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”. Strasbourg.

7.AEPD, PFPDT. (2009). International Standards on the Protection of Personal Data and Privacy, ***Madrid Resolution***. In *International Conference of Data Protection and Privacy Commissioners,* Agencia Española de Protección de Datos (AEPD) and Préposé fédéral à la protection des données et à la transparence (PFPDT), Madrid. Διαθέσιμο στο: https://edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_en.pdf

8.Ahmadi, S. (2019). *5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards*. Academic Press.

9.Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). What will 5G be?. *IEEE Journal on selected areas in communications*, *32*(6), 1065-1082.

10. APEC. (2019). Cross-Border Privacy Rules System Policies, Rules and Guidelines. Διαθέσιμο στο: http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

11. APEC. (2015). APEC Privacy Framework. Singapore: APEC. Διαθέσιμο στο: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

12. Araujo, T., Helberger, N., Kruikemeier, S., & De Vreese, C. H. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & SOCIETY*, *35*(3), 611-623.

13. Article 29 Data Protection Working Party. (2014). "Opinion 05/2014 on Anonymisation Techniques".WP216. Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4

14. Article 29 Data Protection Working Party. (2018). "Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data." WP264. Διαθέσιμο στο: https://edpb.europa.eu/our-work-tools/our-documents/recommendation-standard-application-form-approval-controller-binding_en

15. Article 29 Working Party. (1998). "Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive". Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

16. Article 29 Working Party. (2003). "Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers". Διαθέσιμο στο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf

17. Article 29 Working Party. (2006). "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)". Διαθέσιμο στο: http://www.dataprotection.ro/servlet/ViewDocument?id=234

18. Article 29 Working Party. (2010). "Opinion 1/2010 on the concepts of "controller" and "processor". Διαθέσιμο στο:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

19. Article 29 Working Party. (2013). "Opinion 02/2013 on apps on smart devices". WP202. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/news-overview.cfm

20. Article 29 Working Party. (2018). "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679," WP 251. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

21. Article 29 Working Party. (2018). "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679," WP 250. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

22. Article 29 Working Party. (2018). "Guidelines on Personal data breach notification under Regulation 2016/679". Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

23. Article 29 Working Party. (2018). "Guidelines on transparency under Regulation 2016/679". WP260. Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

24. Article 29 Working Party. (2018). "Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR". Διαθέσιμο στο: https://ec.europa.eu/newsroom/article29/items/623850/en

25. Asinari, M. V. P. (2002). Is There any Room for Privacy and Data Protection within the WTO Rules?, *Elec. Comm'n L. Rev., 9*, 249.

26. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, vol. 54, 15*, 2787-2805.

27. Bădică, C., Brezovan, M., & Bădică, A. (2013). An Overview of Smart Home Environments: Architectures, Technologies and Applications. *BCI*.

28. Bargiotti, L., Gielis, I., Verdegem, B., Breyne, P., Pignatelli, F., Smits, P., & Boguslawski, R. (2016). *Guidelines for public administrations on location privacy: European Union Location Framework* (No. JRC103110). Joint Research Centre (Seville site).

29.Barnes, R., Winterbottom, J., & Dawson, M. (2011). Internet geolocation and location-based services. *IEEE Communications Magazine*, *49*(4), 102-108.

30.Berrezueta-Guzman, J., Pau, I., Martín-Ruiz, M. L., & Máximo-Bocanegra, N. (2020). Smart-home environment to support homework activities for children. *IEEE Access*, *8*, 160251-160267.

31.Bianchi, D., & Tosun, O. K. (2018). *Cyber Attacks and Stock Market Activity. SSRN Electronic Journal.*

32.Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016, September). A process for data protection impact assessment under the european general data protection regulation. In *Annual Privacy Forum* (pp. 21-37). Springer, Cham.

33.Bigelow, R. (1979). Transborder data flow barriers. *Jurimetrics J.*, *20*, 8.

34.Blackman, C., Forge, S. (Scientific and Quality of Life Policies Directorate-General for Internal Policies Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies). (2019). "5G Deployment: State of play in Europe, USA and Asia". Διαθέσιμο στο : https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2019)631060

35.Body of European Regulators for Electronic Communications. (2019). "Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem". Διαθέσιμο στο: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8910-report-on-the-impact-of-5g-on-regulation-and-the-role-of-regulation-in-enabling-the-5g-ecosystem

36.Bottis, M., Panagopoulou-Koutnatzi, F., Michailaki, A., & Nikita, M. (2019). The right to access information under the GDPR. *International Journal of Technology Policy and Law*, *3*(2), 131-142.

37.Bugeja, J. (2021). On privacy and security in smart connected homes.

38.Bugeja, J., & Jacobsson, A. (2019, August). On the Design of a Privacy-Centered Data Lifecycle for Smart Living Spaces. In *IFIP International Summer School on Privacy and Identity Management* (pp. 126-141). Springer, Cham.

39.Burton, C., De Boel, L., Kuner, C., Pateraki, A., Cadiot, S., & Hoffman, S. G. (2016). The final european union general data protection regulation. *BNA Privacy & Security Law Report, 15*, 153.

40.Casalini, F., & González, J. L. (2019). Trade and cross-border data flows.

41.Chen, J., Edwards, L., Urquhart, L., & McAuley, D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *Reconsidering Joint Controllership and the Household Exemption (November 18, 2019). International Data Privacy Law*.

42.Chen, X., Li, Z., Chen, Y., & Wang, X. (2019). Performance analysis and uplink scheduling for QoS-aware NB-IoT networks in mobile computing. *IEEE Access*, *7*, 44404-44415.

43.Cockfield, A. J. (2015). Bid Data and Tax Haven Secrecy. *Fla. Tax Rev.*, *18*, 483.

44.Cockfield, A. J. (2019). Sharing Tax Information in the 21st Century: Big Data Flows and Taxpayers as Data Subjects. *Canadian Tax Journal*, *67*(4), 1179-1199.

45.Commission Implementing Decision Of 28.6.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. Διαθέσιμο στο: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf

46.Commission Nationale de l'Informatique et des Libert´es (CNIL). (2018). "Privacy Impact Assessment: Methodology". February 2018 edition. Διαθέσιμο στο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

47.Committee of Ministers of the Council of Europe. (1999). Σύσταση R (99) 5 on the protection of privacy on the Internet. Διαθέσιμο στο: https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines

48.Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). (2018). Διαθέσιμο στο: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents.

49.Council of Europe, Consultative Committee of Convention 108. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01. Strasbourg. Διαθέσιμο στο: https://rm.coe.int/16806ebe7a

50.Council of Europe. (2018). *Handbook on European data protection law*. Luxembourg: European Union Agency for Fundamental Rights and Council of Europe.

51.Council of the European Union. (2019) "Note entitled: Law enforcement and judicial aspects related to 5G," Διαθέσιμο στο: http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf

52.Council of the European Union. (2019). Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G-Council Conclusions (14517/19). Brussels. Διαθέσιμο στο: https://www.consilium.europa.eu/en/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/

53.Council, N. C. (2016). Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys. *Oslo, NCC*.

54.Cradock, E., Stalla-Bourdillon, S., & Millard, D. (2017). Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform. *Computer law & security review*, *33*(2), 142-158.

55.De Goede, M. (2012). The SWIFT affair and the global politics of European security. *JCMS: Journal of Common Market Studies*, *50*(2), 214-230.

56.Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]. Διαθέσιμο στο: https://www.efta.int/sites/default/files/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/2018%20-%20English/154-2018.pdf

57.Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication Services) to the EEA Agreement. Διαθέσιμο στο:

https://www.efta.int/media/documents/legal-texts/eea/other-legal-documents/adopted-joint-committee-decisions/1999%20-%20English/083-1999.pdf

58.ECOWAS. (2010). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, adopted at the 37th session of the Authority of ECOWAS Heads of State and Government, (Abuja, 16 February 2010).

59.EDPB (European Data Protection Board). (2020). Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.0. Διαθέσιμο στο: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

60.EDPB, EDPS. (2019). "Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection". Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en

61.Enterprivacy Consulting Group. (2017). Categories of Personal Information. Διαθέσιμο στο: https://iapp.org/resources/article/categories-of-personal-data/

62.European Central Bank, "Euro foreign exchange reference rates." Διαθέσιμο στο: https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/eurofxref-graph-sek.en.html

63.European Commission. (2019). "Commission Recommendation on Cybersecurity of 5G networks C 2335 final". Διαθέσιμο στο: https://eur-lex.europa.eu/eli/reco/2019/534/oj

64.European Commission. (2019). Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union. Brussels. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN

65.European Commission. (2021). Intensifying Negotiations on transatlantic Data Privacy Flow. Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443

66.European Commission. Adequacy decisions. Διαθέσιμο στο: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

67.European Data Protection Board, European Data Protection Supervisor. (2019). Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI). Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-opinion-ehdsi_en

68.European Data Protection Board. (2019). "Statement 01/2019 on the US Foreign Account Tax Compliance Act (FATCA)." Διαθέσιμο στο: https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12-25-fatca_statement_en.pdf

69.European Data Protection Supervisor. (2020). Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling. Διαθέσιμο στο: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and_en

70.European Economic Area (EEA),"Relations with the EU". Διαθέσιμο στο: https://www.efta.int/eea

71.European Parliament legislative resolution of 11 February 2010 on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme (05305/1/2010 REV 1 — C7-0004/2010 — 2009/0190(NLE)) P7_TA(2010)0029.

72.European Union Agency for Network and Information Security. (2019) "Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default". Διαθέσιμο στο: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2

73.Farhang, S., Hayel, Y., & Zhu, Q. (2015, September). PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks. In *2015 IEEE Conference on Communications and Network Security (CNS)* (pp. 263-271). IEEE.

74.Federal Trade Commission. (2020). "Complying with COPPA: frequently asked questions." Διαθέσιμο στο: https://www.ftc.gov/tips-

advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

75.Ferracane, M. (2017). Restrictions on Cross-Border data flows: a taxonomy.

76.Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, *101*, 55-82.

77.Fishman, W. L. (1980). Introduction to transborder data flows. *Stan. J. Int'l L.*, *16*, 1.

78.GATS, Annex 1B to the 1994 Marrakesh Agreement on Establishing the World Trade Organization (WTO Agreement).

79.Ge, X., Tu, S., Mao, G., Wang, C. X., & Han, T. (2016). 5G ultra-dense cellular networks. *IEEE Wireless Communications*, *23*(1), 72-79.

80.Gerke, S., Shachar, C., Chai, P. R., & Cohen, I. G. (2020). Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nature medicine*, *26*(8), 1176-1182.

81.Giurgiu, A., & Lallemang, T. (2017). The General Data Protection Regulation: a new opportunity and challenge for the banking sector. *Ace Magazine et Archives Online: Fiscalité, Comptabilité, Audit, Droit des Affaires au Luxembourg*, *1*, 3-15.

82.Goudos, S. K., Deruyck, M., Plets, D., Martens, L., Psannis, K. E., Sarigiannidis, P., & Joseph, W. (2019). A novel design approach for 5G massive MIMO and NB-IoT green networks using a hybrid Jaya-differential evolution algorithm. *IEEE Access*, *7*, 105687-105700.

83.Goudos, S. K., Yioultsis, T. V., Boursianis, A. D., Psannis, K. E., & Siakavara, K. (2019). Application of new hybrid Jaya grey wolf optimizer to antenna design for 5G communications systems. *IEEE Access*, *7*, 71061-71071.

84.Greenleaf, G., & Georges, M. (2014). African regional privacy instruments: Their effects on harmonization.

85.Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE access*, *3*, 1206-1232.

86.Gurusamy, S. (2009). *Financial services and system*. Tata McGraw-Hill Education Private Limited.

87.Hall, H. K. (2018). Restoring dignity and harmony to united states-european union data protection regulation. *Communication Law and Policy*, *23*(2), 125-157.

88.Hassan, Q. F. (Ed.). (2018). *Internet of things A to Z: technologies and applications*. John Wiley & Sons.

89.Helvacioglu, A. D., & Stakheyeva, H. (2017). The tale of two data protection regimes: The analysis of the recent law reform in Turkey in the light of EU novelties. *Computer law & security review*, *33*(6), 811-824.

90.Hendrik Mildebrath, European Parliamentary Research Service. (2020). The CJEU judgment in the Schrems II case. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)652073

91.HIPSSA–Data Protection: SADC Model Law. (2013). Διαθέσιμο στο: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

92.Hiroyuki, T. (2021). Japan updates enforcement rules for amended APPI. Διαθέσιμο στο: https://iapp.org/news/a/japan-updates-enforcement-rules-for-amended-appi/

93.Hondius, F. (1974). International Data Protection Action. In *Policy Issues in Data Protection and Privacy Policy Issues in Data Protection and Privacy*.

94.Hošek, J. (2016). *Enabling Technologies and User Perception Within Integrated 5G-IoT Ecosystem*. Vysoké učení technické v Brně, nakladatelství VUTIUM.

95.Ibrahim, M. D., Hocaoglu, M. B., Numan, B., & Daneshvar, S. (2018). Estimating efficiency of Directive 2011/24/EU cross-border healthcare in member states. *Journal of comparative effectiveness research*, *7*(8), 827-834.

96.Information Commissioner's Office. (2020). "Age appropriate design: a code of practice for online services". Διαθέσιμο στο: https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

97.Information Commissioner's Office. Data Protection and the EU. Διαθέσιμο στο: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu

98.Information Commissioner's Office. International transfers after the UK exit from the EU Implementation Period. Διαθέσιμο στο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

99.ISO/IEC 27701:2019. Security techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirements and guidelines. Διαθέσιμο στο: https://www.iso.org/standard/71670.html

100.Italian Data Protection Authority (Garante per la protezione dei dati personali). (2021). "Tik Tok: Italian SA imposes limitation on processing after the death of the girl from Palermo," Διαθέσιμο στο: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524224

101.Italian Data Protection Authority (Garante per la protezione dei dati personali). (2020). "Tik Tok Endangers Children's Privacy: Italian Dpa Initiates Proceedings Against the Social Network," Διαθέσιμο στο: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923

102.Kakalou, I., Psannis, K. E., Krawiec, P., & Badea, R. (2017). Cognitive radio network and network service chaining toward 5G: Challenges and requirements. *IEEE Communications Magazine*, *55*(11), 145-151.

103.Karaduman, O. (2017). The general data protection regulation: Achieving compliance for EU and non-EU companies. *Bus. L. Int'l*, *18*, 225.

104.Karyda, M., & Mitrou, L. (2016). Data Breach Notification: Issues and Challenges for Security Management. In *MCIS* (p. 60).

105.Khorev, P., & Chernetsov, A. (2020). The Problem of Ensuring Cross-border Personal Data Transfer and Methods for Its Solving. In *2020 V International Conference on Information Technologies in Engineering Education (Inforino)* (pp. 1-4). IEEE.

106.King, N. (2003). Smart home–a definition. *Intertek Research and Testing Center*.

107.Kirby, M. (2011). The history, achievement and future of the 1980 OECD guidelines on privacy. *International Data Privacy Law*, *1*(1), 6-14.

108.Kişisel Verileri Koruma Kurumu, KVKK. (2019). Data Protection in Turkey. Διαθέσιμο στο: https://www.kvkk.gov.tr/Search?keyword=data%20protection%20in%20turkey&langText=en

109.Koivisto, M., Hakkarainen, A., Costa, M., Kela, P., Leppanen, K., & Valkama, M. (2017). High-efficiency device positioning and location-aware communications in dense 5G networks. *IEEE Communications Magazine*, *55*(8), 188-195.

110.Korb, K. B., & Nicholson, A. E. (2010). *Bayesian artificial intelligence*. CRC press.

111.Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, No. 187. OECD Publishing.

112.Kuner, C. (2013). *Transborder data flows and data privacy law*. OUP Oxford.

113.Kuner, C. (2020). The Schrems II judgment of the Court of Justice and the future of data transfer regulation. Διαθέσιμο στο: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

114.Kuner, C. (2021). Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. *University of Cambridge Faculty of Law Research Paper*, (20).

115.Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected Articles. Update of Selected Articles (May 4, 2021).

116.Kuner, C., Bygrave, L., Docksey, C., Svantesson, D., & de Terwagne, C. (2018). 2018 Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019).

117.Kuner, C., Docksey, C., & Bygrave, L. (2020). *The EU General Data Protection Regulation: A Commentary*. Oxford University Press.

118.Latva-aho, M., Leppänen, K., Clazzer, F., & Munari, A. (2020). Key drivers and research challenges for 6G ubiquitous wireless intelligence.

119.Lemstra, W. (2018). Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implications. *Telecommunications Policy*, *42*(8), 587-611.

120.Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y. J. A. (2019). The roadmap to 6G: AI empowered wireless networks. *IEEE Communications Magazine*, *57*(8), 84-90.

121.Leung, R. (2018). Cross-border data transfers under the GDPR: a perspective from non-European e-commerce businesses.

122.Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1-9.

123.Liapakis, X. (2018). A GDPR Implementation Guide for the Insurance Industry. *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, *7*(4), 34-44.

124.Lichtblau, E., & Risen, J. (2006). Bank data is sifted by US in secret to block terror. *New York Times*, *23*, 66-205.

125.Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *A comprehensive guide to 5G security*. New York: John Wiley & Sons.

126.Liyanage, M., Salo, J., Braeken, A., Kumar, T., Seneviratne, S., & Ylianttila, M. (2018, July). 5G privacy: Scenarios and solutions. In *2018 IEEE 5G World Forum (5GWF)* (pp. 197-203). IEEE.

127.Loideain, N. N. (2019). A port in the data-sharing storm: the GDPR and the Internet of things. *Journal of Cyber Policy*, *4*(2), 178-196.

128.López-González, J., Casalini, F., & Nemoto, T. (2021). Mapping approaches to cross-border data flows. *Addressing Impediments to Digital Trade*.

129.Majcher, I. (2020). The Schengen-wide entry ban: how are non-citizens' personal data protected?. *Journal of Ethnic and Migration Studies*, 1-17.

130.Makulilo, A. B. (Ed.). (2016). *African data privacy laws* (Vol. 33). Cham: Springer.

131.Martina, D. (2017). EU-USA cooperation on information sharing in the fight against terrorism: the roles of privacy and security, and the cases of the TFTP and PNR agreements.

132. Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

133. McGeveran, W., & Schmitz, C. (2020). General-Purpose Privacy Regulation and Translational Genomics. *The Journal of Law, Medicine & Ethics*, *48*(1), 142-150.

134. McKinsey Global Institute (2016). Digital Globalization: The New Era of Global Flow. Διαθέσιμο στο: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows

135. Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B. G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems*, *83*, 619-628.

136. Mildebrath, H. European Parliamentary Research Service. (2020). The CJEU judgment in the Schrems II case. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2020)652073

137. Milossi, M., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2021). AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach. *IEEE Access*, *9*, 58455-58466.

138. Milt, K. (2017). Personal data protection. Fact Sheets on the European Union. Διαθέσιμο στο: https://www.europarl.europa.eu/thinktank/en/search.html?authors=28691

139. Mishra, N. (2020). Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?. *World Trade Review*, *19*(3), 341-364.

140. Möller, C. (2017). *The Evolution of Data Protection and Privacy in the Public Security Context-An Institutional Analysis of Three EU Data Retention and Access Regimes* (Doctoral dissertation, Queen Mary University of London).

141. Mulder, T., & Tudorica, M. (2019). Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law*, *28*(3), 261-274.

142. Nguyen, D., & Paczos, M. (2020). Measuring the economic value of data and cross-border data flows: A business perspective. Διαθέσιμο στο: https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en

143. Ni, J., Lin, X., & Shen, X. S. (2018). Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE Journal on Selected Areas in Communications*, *36*(3), 644-657.

144. Nicholson, J.R., & Noonan, R. (2014). Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services. U.S. Department of Commerce. Διαθέσιμο στο: https://www.commerce.gov/sites/default/files/migrated/reports/digitaleconomyandcross-bordertrade.pdf

145. NIS Cooperation Group. (2019). "EU coordinated risk assessment of the cybersecurity of 5G networks". Διαθέσιμο στο: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

146. NIS Cooperation Group. (2020). Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. Διαθέσιμο στο: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

147. Norwegian Data Protection Authority. (2020). "Final decision, administrative fine for Rælingen municipality,"Διαθέσιμο στο: https://www.datatilsynet.no/en/news/2020/final-decision-administrative-fine-for-ralingen-municipality/

148. Ntouvas, I. (2019). Exporting personal data to EU-based international organizations under the GDPR. *International Data Privacy Law*, *9*(4), 272-284.

149. Nurse, J. R., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. *IT professional*, *19*(5), 20-26.

150. Nurse, J. R., Radanliev, P., Creese, S., & De Roure, D. (2018). If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems.

151. OAS. (2015). Protection of Personal Data. Διαθέσιμο στο: http://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf

152. OECD. (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Διαθέσιμο στο:

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

153. OECD. (2013). *Introduction to Data and Analytics (Module 1): Taxonomy, Data Governance Issues, and Implications for further Work*.

154. OECD. (2013). Guidelines governing the protection of privacy and transborder flows of personal data. Διαθέσιμο στο: https://edps.europa.eu/data-protection/data-protection/legislation_en

155. OECD. (2015). *Data-driven innovation: Big data for growth and well-being*.

156. OECD. (2020). Mapping approaches to cross-border data flows. Report for the G20 Digital Economy Task Force. Διαθέσιμο στο: https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf?expires=1620464835&id=id&accname=guest&checksum=BCE1CCC78F3747D1386E1D0446E3B8CC

157. OECD/IDB. (2016). Broadband Policies for Latin America and the Caribbean: A Digital Economy Toolkit. Διαθέσιμο στο: http://dx.doi.org/10.1787/9789264251823-en

158. Office of the Privacy Commissioner. (2021). A quick tour of the privacy principles. Διαθέσιμο στο: https://www.privacy.org.nz/privacy-act-2020/privacy-principles/the-privacy-principles/

159. OneTrust DataGuidance, Baptista Luz Advogados. (2020). Comparing privacy laws: GDPR v. LGPD.

160. Orji, U. J. (2017). Regionalizing data protection law: a discourse on the status and implementation of the ECOWAS Data Protection Act. *International Data Privacy Law*, *7*(3), 179-189.

161. Partnering with the Industry for 5G Security Assurance. (2019). Huawei White Paper, Shenzhen, China.

162. Patel, O., & Lea, N. (2020). EU-US Privacy Shield, Brexit and the Future of Transatlantic Data Flows. *Available at SSRN 3618937*.

163. Pernot-Leplay, E. (2020). China's Approach on Data Privacy Law: A Third Way Between the US and the EU?. *Penn St. JL & Int'l Aff.*, *8*, 49.

164. Piper, D. L. A. (2021). *Data protection laws of the world: full handbook*. DLA Piper.

165. Polčák, R. (2017). Stock Exchange Interconnections and Legal Issues in Data Exchange. *Masaryk University Journal of Law and Technology*, *11*(2), 351-362.

166. Prasad, A. R., Zugenmaier, A., Escott, A. & Soveri, M. C. (2018). "3GPP 5G security". Διαθέσιμο στο : http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g?from=timeline

167. Privacy Commissioner of Canada. (2009). Guidelines for Processing Personal Data Across Borders. Διαθέσιμο στο: https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/.

168. Raducu, I. (2014). Reflections Upon the Interaction between Domestic and European Personal Data Protection Legislation. *University of Luxembourg Law Working Paper*, (2014-05).

169. Report of the Appellate Body. Διαθέσιμο στο: https://www.wto.org/english/tratop_e/dispu_e/161-169abr_e.pdf

170. Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020, October). Taxonomy about the Stages of Performing Automated Decision-Making Processing under GDPR in the Light of 6G Networks. In *2020 3rd World Symposium on Communication Engineering (WSCE)* (pp. 23-27). IEEE.

171. Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR interference with next generation 5G and IoT networks. *IEEE Access*, *8*, 108052-108061.

172. Rizou, S., Alexandropoulou-Egyptiadou, E., Ishibashi, Y. & Psannis, K. E. (2022). Preserving Minors' Data Protection in IoT-based Smart Homes According to GDPR Considering Cross-Border Issues. *Journal of Communications*, *17*(3), 180-187.

173. Robinson, D. (2016). Facebook data transfers threatened by EU ruling. *Financial Times*. Διαθέσιμο στο: https://www.ft.com/content/8fe7c850-226f-11e6-9d4d-c11776a5124d

174. Russell, S. J., & Norvig, P. (2003). edn: *Artificial intelligence: a modern approach*.

175. Russell, S. J., & Norvig, P. (2009). *Artificial intelligence: a modern approach*. Prentice Hall.

176. Sanchez, J. L. C., Bernabe, J. B., & Skarmeta, A. F. (2018). Towards privacy preserving data provenance for the Internet of Things. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 41-46). IEEE.

177. Scassa, T. (2020). Data Protection and the Internet: Canada. In *Data Protection in the Internet* (pp. 55-76). Springer, Cham.

178. Schwartz, P. M. (2008). Preemption and privacy. *Yale Lj*, *118*, 902-947.

179. Skarmeta, A. F., Hernandez-Ramos, J. L., & Moreno, M. V. (2014). A decentralized approach for security and privacy challenges in the internet of things. In *2014 IEEE world forum on Internet of Things (WF-IoT)* (pp. 67-72). IEEE.

180. Sovacool, B. K., & Del Rio, D. D. F. (2020). Smart home technologies in Europe: a critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews*, *120*, 109663.

181. Spiezia, V. (2020). International agreements on cross-border data flows and international trade: A statistical analysis.

182. Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, *19*, 174-184.

183. Sullivan, C. (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. *Computer Law & Security Review*, *35*(4), 380-397.

184. Swedish Authority for Privacy Protection. (2020) "Serious deficiencies in the Stockholm online School Platform," Διαθέσιμο στο: https://www.imy.se/en/news/serious-deficiencies-in-the-stockholm-online-school-platform/

185. Swedish National Board of Trade. (2014). No Transfer, No Trade– the Importance of Cross-Border Data Transfers for Companies Based in Sweden. Διαθέσιμο στο: https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf

186. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

187. Tracol, X. (2021). Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and

international organisations. In *ERA Forum* (pp. 1-16). Springer Berlin Heidelberg.

188. Trans-Pacific Partnership Agreement (TPP). (2016). Διαθέσιμο στο: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents

189. Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation?. In *Institutionalisation beyond the Nation State*. Springer, Cham, (pp. 55-74).

190. UNCTAD (2019). Value Creation and Capture: Implications for Developing Countries. Digital Economy Report. Διαθέσιμο στο: https://unctad.org/webflyer/digital-economy-report-2019

191. United Nations. (1990). The guidelines concerning computerized personal data files.

192. United States Department of Commerce. (2020). "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II". Διαθέσιμο στο: https://www.commerce.gov/sites/default/files/202009/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

193. US Department of Commerce. (2016). Measuring the Value of Cross-Border Data Flows. Διαθέσιμο στο: https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf

194. Vemou, K., & Karyda, M. (2019). Evaluating privacy impact assessment methods: guidelines and best practice. *Information & Computer Security*.

195. Ventrella, E. (2020). Privacy in emergency circumstances: data protection and the COVID-19 pandemic. In *ERA Forum* (Vol. 21, No. 3, pp. 379-393). Springer Berlin Heidelberg.

196. Verizon. (2020) Data Breach Investigations Report. Διαθέσιμο στο: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

197. Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, *29*, 485-532.

198. Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. *American Business Law Journal*, *56*(2), 287-344.

199.Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?. *International Data Privacy Law*, 8, 318–337.

200.Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law*. Springer Nature.

201.Wang, M., & Jiang, Z. (2017). The defining approaches and practical paradox of sensitive data: An investigation of data protection laws in 92 countries and regions and 200 data breaches in the world. *International Journal of Communication*, *11*, 20.

202.Weber, R. H. (2012). Regulatory autonomy and privacy standards under the GATS. *Asian J. WTO & Int'l Health L & Pol'y*, *7*, 25.

203.Weber, R. H. (2013). Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. *International Data Privacy Law*, *3*(2), 117-130.

204.Weber, R. H., & Staiger, D. (2017). *Transatlantic data protection in practice*. Basel. Springer.

205.Whitman, J. Q. (2003). The two western cultures of privacy: Dignity versus liberty. *Yale LJ*, *113*, 1151.

206.Wigand, R. T., Shipley, C., & Shipley, D. (1984). Transborder data flow, informatics, and national policies. *Journal of Communication*, *34*(1), 153-175.

207.Wolters, P. T. J. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility?. *International Data Privacy Law*, *7*(3), 165-178.

208.WTO. (2000). Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef- AB-2000-8.

209.WTO. (2005). United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body. Διαθέσιμο στο: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(%40Symbol%3d+wt%2fds285%2f*)&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true

210.Xiao, Z., & Zeng, Y. (2020). An overview on integrated localization and communication towards 6G. *arXiv preprint arXiv:2006.01535*.

211. Yakovleva, S. (2020). Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'. *The Journal of World Investment & Trade*, *21*(6), 881-919.

212. Yakovleva, S., & Irion, K. (2016). The Best of Both Worlds-Free Trade in Services and EU Law on Privacy and Data Protection. *Eur. Data Prot. L. Rev.*, *2*, 191.

213. Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: reconciling EU governance of personal data flows with external trade. *International Data Privacy Law*, *10*(3), 201-221.

214. Yin, C., Xi, J., Sun, R., & Wang, J. (2017). Location privacy protection based on differential privacy strategy for big data in industrial internet of things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3628-3636.

215. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., Nguyen, T.H., Liu, F., Hewa, T., Liyanage, M. & Ijaz, A. (2020). 6g white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*.

216. Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. *Seton Hall L. Rev.*, *47*, 995.

217. Zhang, G., Fan, D., Zhang, Y., Li, X., & Liu, X. (2015). A privacy preserving authentication scheme for roaming services in global mobility networks. *Security and Communication Networks*, *8*(16), 2850-2859.

218. Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-20.

219. Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. *The International Journal of Human Rights*, *24*(10), 1572-1593.

ΑΝΑΦΟΡΕΣ ΝΟΜΟΛΟΓΙΑΣ (με αύξουσα χρονολογική σειρά)

C-101/01. Απόφαση του ΔΕΚ της 6ης Νοεμβρίου 2003, Ποινική δίκη κατά Bodil Lindqvist.

C-317/04, C-318/04. Απόφαση του ΔΕΚ (τμήμα μείζονος συνθέσεως) της 30ης Μαΐου 2006, Ευρωπαϊκό Κοινοβούλιο κατά Συμβουλίου της Ευρωπαϊκής Ενώσεως (C-317/04) και Επιτροπή των Ευρωπαϊκών Κοινοτήτων (C-318/04).

C-293/12. CJEU. Judgment of the Court (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.

C-131/12. CJEU. Judgment of the Court (Grand Chamber) of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

C-141/12, C-372/12. CJEU. Judgment of the Court (Third Chamber) of 17 July 2014, YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S.

C-212/13. CJEU, Judgment of the Court (Fourth Chamber) of 11 December 2014, František Ryneš v Úřad pro ochranu osobních údajů.

C-201/14. Απόφαση του ΔΕΕ (τρίτο τμήμα) της 1ης Οκτωβρίου 2015, Smaranda Bara κ.λπ. κατά Casa Naţională de Asigurări de Sănătate κ.λπ.

C-362/14. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 6ης Οκτωβρίου 2015, Maximillian Schrems κατά Data Protection Commissioner.

C-311/18. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 16ης Ιουλίου 2020, Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems.

C-645/19. Απόφαση του ΔΕΕ (τμήμα μείζονος συνθέσεως) της 5ης Ιουνίου 2021, Facebook Ireland Ltd, Facebook Inc, Facebook Belgium BVBA κατά Gegevensbeschermingsautoriteit.

Γνωμοδότηση Εισ. ΑΠ 8/2018

ΑΠΔΠΧ. Αρ. Απόφασης 109/31-03-1999, η οποία επαναλήφθηκε με την Αρ. Απόφασης 24/2004, (ΦΕΚ Β΄ 684/11-05-2004)

ΑΠΔΠΧ. Αρ. Απόφασης 523/19-10-1999, η οποία επαναλήφθηκε με την Αρ. Απόφασης 25/2004, (ΦΕΚ Β΄ 684/11-05-2004)

ΑΠΔΠΧ. Αρ. Απόφασης 86/2002

ΑΠΔΠΧ. Αρ. Απόφασης 152/2013

ΑΠΔΠΧ. Αρ. Απόφασης 56/2015

ΑΠΔΠΧ. Αρ. Απόφασης 81/2017

ΑΠΔΠΧ. Αρ. Απόφασης 87/2017

ΑΠΔΠΧ. Αρ. Απόφασης 65/2018 (ΦΕΚ 1622/Β/10-5-2019)

ΑΠΔΠΧ. Αρ. Απόφασης 18/2019

ΚΥΡΙΟΤΕΡΕΣ ΙΣΤΟΣΕΛΙΔΕΣ

https://www.europarl.europa.eu

https://www.oxfordlearnersdictionaries.com

https://www.dpa.gr

https://www.oecd.org

https://www.aade.gr

http://www.tiresias.gr

https://www.doingbusiness.org

https://www.wto.org

https://eurlex.europa.eu

https://ec.europa.eu

https://www.coe.int

https://www.enisa.europa.eu

https://www.apec.org

http://cbprs.org

https://www.ecowas.int

https://www.sadc.int

http://www.itu.int

https://www.oas.org

https://www.abf.gov.au

https://unctad.org

https://popia.co.za

https://laws-lois.justice.gc.ca

https://pd.rkn.gov.ru

http://www.jus.gob.ar

https://www.legislation.gov.au

https://www.privacy.org

https://www.legislation.govt.nz

http://www.hellenicpolice.gr

https://www.efta.int/eea

https://www.swift.com

https://www.autoriteitpersoonsgegevens.nl

http://www.dataprotection.gov.cy

https://www.congress.gov

https://www.nsa.gov

https://www.consilium.europa.eu

https://www.gov.uk

https://ico.org.uk

https://www.kodiko.gr/

Οι ηλεκτρονικές πηγές προσπελάστηκαν στις 24/01/2022