ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της Ηλιάνας Κοντογεώργου (Α.Μ.: ΜΔΙ2217)

Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ: ΗΠΑ, BRUSSELS EFFECT ΚΑΙ ΔΙΑΣΥΝΟΡΙΑΚΗ ΡΟΗ

PERSONAL DATA PROTECTION OUTSIDE THE EU: USA, BRUSSELS EFFECT & CROSS-BORDER FLOW

Επιβλέπουσα:

Λίλιαν Μήτρου

Πειραιάς, Αύγουστος 2024

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εξετάζει το ζήτημα της προστασίας προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης. Αρχικά, περιγράφεται συνοπτικά το νομοθετικό πλαίσιο που έχει υιοθετηθεί στην Ευρωπαϊκή Ένωση καθώς και οι προσεγγίσεις που έχουν ακολουθηθεί από κράτη εκτός ΕΕ. Στη συνέχεια, η εργασία επικεντρώνεται στο καθεστώς που ισχύει στις ΗΠΑ και εξετάζεται η ιστορική εξέλιξη της προστασίας προσωπικών δεδομένων στις Ηνωμένες Πολιτείες, το νομικό πλαίσιο και οι διαφορές αυτού με το πλαίσιο της ΕΕ. Έπειτα, παρουσιάζεται η έννοια και οι προϋποθέσεις εμφάνισης του «Brussels Effect», και αναφέρονται ειδικότερα παραδείγματα για την επίδραση του GDPR στις νομοθεσίες άλλων κρατών εκτός ΕΕ και στις πρακτικές επιχειρήσεων που δραστηριοποιούνται διεθνώς. Επιπροσθέτως, εξετάζεται η διασυνοριακή ροή προσωπικών δεδομένων, με έμφαση στο ρυθμιστικό πλαίσιο που έχει υιοθετηθεί και στις διαβιβάσεις δεδομένων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες Αμερικής. Τέλος, παρατίθενται τα συμπεράσματα που αποκομίζονται από την ανάλυση της εργασίας, επισημαίνεται η σημασία της προστασίας προσωπικών δεδομένων στον σύγχρονο κόσμο και γίνεται αναφορά στις προοπτικές και τις μελλοντικές εξελίξεις στον τομέα της προστασίας δεδομένων εκτός ΕΕ.

ABSTRACT

This thesis examines the issue of personal data protection outside the European Union. First, it succinctly describes the legislative framework adopted in the European Union, as well as the approaches that have been followed by non-EU countries. In the subsequent section, the dissertation delves into the regime in place in the United States and explores the historical evolution of data protection in the United States, the legal framework, and its differences with the EU framework. Then, the concept and conditions for the occurrence of the "Brussels Effect" are presented and specific examples of the impact of GDPR on legislation in non-EU countries and the practices of internationally operating businesses are provided. Furthermore, the cross-border flow of personal data is explored, with a focus on the regulatory framework adopted and on data transfers from the European Union to the United States of America. Eventually, the conclusions drawn from the preceding analysis are presented, the significance of data protection in the modern world is highlighted, and the prospects and future developments in the field of data protection outside the EU are discussed.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΕΠ	Ακαθάριστο Εγχώριο Προϊόν
ΑΠΔ	Αρχές Προστασίας Δεδομένων
ΔΕΕ	Δικαστήριο Ευρωπαϊκής Ένωσης
ΕΕ	Ευρωπαϊκή Ένωση
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΧΘΔ	Χάρτης Θεμελιωδών Δικαιωμάτων
ASEAN	Association of Southeast Asian Nations
ATDS	Automatic Telephone Dialing System
APEC	Asia-Pasific Economic Cooperation
APPs	Australian Privacy Principles
APPI	Act on the Protection of Personal Information
BCR	Binding Corporate rules
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography And Marketing
CBPR	Cross-Border Privacy Rules
CCPA	California Consumer Privacy Act
CFPB	Consumer Financial Protection Bureau
CLS	Cybersecurity Law of China
COPPA	Children's Online Privacy Protection Act
CPA	Colorado Privacy Act
CPRA	California Privacy Rights Act
DMF	Digital Management Framework
DPC	Data Protection Commission of Ireland
DPRC	Data Protection Review Court
DSL	Data Security Law

EDPB	European Data Protection Board
FACTA	Fair and Accurate Credit Transactions Act
FCRA	Fair Credit Reporting Act
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Biley Act
HHS	United States Department of Health and Human Services
HIPPA	Health Insurance Portability and Accountability Act
LGPD	Brazilian General Data Protection Law
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	Personal Information Protection and Electronic Documents Act
PIPL	China Personal Information Protection Law
POPIA	Protection of Personal Information Act
PPL	Protection of Privacy Law of Israel
PPC	Personal Information Protection Commission of Japan
SCCs	Standard Contractual Clauses
TCPA	Telephone Consumer Protection Act
UNSTAD	UN Trade and Development

1. Εισαγωγή

Η ανάγκη του ανθρώπου να διαφυλάσσεται η ιδιωτικότητά του εμφανίζεται ήδη στα γραπτά του Σωκράτη και άλλων Ελλήνων φιλοσόφων, όταν γίνεται διάκριση, μεταξύ δημόσιου και ιδιωτικού βίου (Moore, 1984). Ωστόσο, το δικαίωμα στην ιδιωτικότητα δεν ήταν πάντοτε αυτονόητο. Η σημαντικότερη εξέλιξη στο δίκαιο της ιδιωτικής ζωής ήταν η δημοσίευση του δικηγόρου Samuel D. Warren και του δικαστή Louis Brandeis με τίτλο «The Right to Privacy» (Bratman, 2002). Οι συγγραφείς Warren και Brandeis στο έργο τους επισημαίνουν ότι οι συνεχώς εξελισσόμενες τεχνολογικές εφευρέσεις και οι νέες επιχειρηματικές μέθοδοι επιτάσσουν την αναγνώριση της προστασίας του προσώπου από την παραβίαση της ιδιωτικότητάς του και την εξασφάλιση στο άτομο του δικαιώματος «να μείνει μόνο του» (Brandeis & Warren, 1890).

Μετά το Β' Παγκόσμιο Πόλεμο, ξεκίνησε πιο γενικευμένη θεωρητική συζήτηση για το δικαίωμα στην ιδιωτική ζωή. Πολυάριθμες δημοσιεύσεις και συγγραφικά έργα αφιερώθηκαν στην περιγραφή της έννοιας της ιδιωτικής ζωής και στην ανάδειξη των προβληματισμών που εγείρονται αναφορικά με την παραβίαση της ιδιωτικής ζωής από την αξιοποίηση των τεχνολογικών εφευρέσεων (Holvast, 2009). Η θεωρητική αυτή συζήτηση σε συνδυασμό με τη ραγδαία εξέλιξη των τεχνολογιών, και ιδίως με την εφεύρεση των ηλεκτρονικών υπολογιστών και των «έξυπνων» συσκευών, καθώς και την ανάπτυξη της τεχνητής νοημοσύνης, οδήγησε σταδιακά στην νομοθετική αναγνώριση του δικαιώματος στην ιδιωτική ζωή και την προστασία των προσωπικών δεδομένων σε πολλά κράτη παγκοσμίως. Κομβικό σημείο για την προστασία των προσωπικών δεδομένων αποτέλεσε η υιοθέτηση του Γενικού Κανονισμού Προστασίας Δεδομένων (γνωστού ως GDPR) στην Ευρωπαϊκή Ένωση, που οδήγησε σε μία νέα εποχή για το δικαίωμα της ιδιωτικότητας και επηρέασε πολλά κράτη εκτός Ευρωπαϊκής Ένωσης.

Ο όρος «προσωπικά δεδομένα» ή «δεδομένα προσωπικού χαρακτήρα» εμφανίζεται στο Γενικό Κανονισμό Προστασίας Δεδομένων. Σύμφωνα με το άρθρο 4 του GDPR «δεδομένα προσωπικού χαρακτήρα» νοούνται ως «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».

Εξάλλου, ο όρος «προσωπικά δεδομένα» δε συναντάται στην αμερικανική νομοθεσία για την προστασία των προσωπικών δεδομένων. Αντιθέτως, γίνεται χρήση διάφορων εννοιών για τον προσδιορισμό των δεδομένων αυτών και συνηθέστερα χρησιμοποιείται ο όρος «Προσωπικές Πληροφορίες» («Personal Information») είτε ο όρος «Πληροφορίες Προσωπικής Ταυτοποίησης» («Personally Identifiable Information»). Η έννοια «Πληροφορίες Προσωπικής Ταυτοποίησης» έχει προσδιοριστεί από το Γραφείο Προστασίας Προσωπικών

Δεδομένων και Ανοιχτής Διακυβέρνησης των ΗΠΑ (Office of Privacy and Open Government)[1], σύμφωνα με το οποίο «Ο όρος Πληροφορίες Προσωπικής Ταυτοποίησης αναφέρεται σε πληροφορίες που μπορούν να χρησιμοποιηθούν για τη διάκριση ή τον εντοπισμό της ταυτότητας ενός προσώπου, όπως το όνομά του, ο αριθμός κοινωνικής ασφάλισης, τα βιομετρικά αρχεία κ.λπ., είτε μόνες τους είτε σε συνδυασμό με άλλες προσωπικές ή ταυτοποιήσιμες πληροφορίες που συνδέονται ή ενδέχεται να συνδεθούν με συγκεκριμένο πρόσωπο, όπως ημερομηνία και τόπος γέννησης, πατρικό όνομα μητέρας κ.λπ.[2]»

Σε νομοθεσίες άλλων χωρών υπάρχουν αντίστοιχοι όροι. Για παράδειγμα, στο Νόμο της Κίνας για την Προστασία Προσωπικών Πληροφοριών (Personal Information Protection Law of the People's Republic of China - PIPL), χρησιμοποιείται ο όρος «Προσωπικές Πληροφορίες» και στο άρθρο 4, προβλέπεται ότι οι προσωπικές πληροφορίες αναφέρονται σε κάθε είδους πληροφορίες που σχετίζονται με ταυτοποιημένα ή ταυτοποιήσιμα φυσικά πρόσωπα και καταγράφονται με ηλεκτρονικά ή άλλα μέσα, εξαιρουμένων των πληροφοριών που ανωνυμοποιούνται. Αντίστοιχα, στο Νόμο της Ιαπωνίας για την Προστασία των Προσωπικών Πληροφοριών (Japan's Act on the Protection of Personal Information - APPI) γίνεται η χρήση του όρου «Προσωπικές Πληροφορίες», που ορίζονται στο άρθρο 2 ως οι πληροφορίες για ένα πρόσωπο εν ζωή που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του εν λόγω προσώπου με βάση το όνομα, την ημερομηνία γέννησης, τον κωδικό αναγνώρισης ή άλλα χαρακτηριστικά.

Τέλος, στο Νόμο του Ισραήλ για την Προστασία της Ιδιωτικότητας (Protection of Privacy Law - PPL), χρησιμοποιείται ο όρος «Προσωπικά Δεδομένα» και ορίζονται στο έβδομο τμήμα ως τα δεδομένα σχετικά με την προσωπικότητα, την προσωπική κατάσταση, τις προσωπικές υποθέσεις, την κατάσταση της υγείας, την οικονομική κατάσταση, τα επαγγελματικά προσόντα, τις απόψεις και τις πεποιθήσεις ενός προσώπου. Ο όρος που χρησιμοποιείται σε κάθε νομοθέτημα και ο προσδιορισμός του όρου αυτού έχει ιδιαίτερη σημασία, καθώς καθορίζει το εύρος της προστασίας που παρέχει η εκάστοτε νομοθεσία, ανάλογα με το αν ο ορισμός που δίδεται είναι ευρύς ή περιορισμένος.

Παρά τη γενική αναγνώριση του δικαιώματος της προστασίας ιδιωτικότητας και των προσωπικών δεδομένων διεθνώς, η προστασία των προσωπικών δεδομένων στη σύγχρονη ψηφιακή εποχή παρουσιάζει σημαντικά ζητήματα, ιδίως δεδομένης της έλλειψης ολοκληρωμένων αυστηρών νομικών πλαισίων σε πολλά κράτη και λόγω της αυξανόμενης διασυνοριακής ροής δεδομένων.

Στόχος της παρούσας διπλωματικής είναι η ειδικότερη ανάλυση των νομικών πλαισίων που έχουν υιοθετηθεί από τα κράτη που βρίσκονται εκτός Ευρωπαϊκής Ένωσης,

[1] Το Γραφείο Προστασίας Προσωπικών Δεδομένων και Ανοιχτής Διακυβέρνησης των ΗΠΑ (Office of Privacy and Open Government, OPOG) αποτελεί τμήμα του Γραφείου του Γενικού Οικονομικού Διευθυντή και του Βοηθού Γραμματέα Διοίκησης.

[2] Privacy, Office of Privacy and Open Government, U.S. Department of Commerce (doc.gov), «Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.», διαθέσιμο εδώ https://www.commerce.gov/opog/it-privacy-policy-office-privacy-and-open-government-us-department-commerce#P126_15356 (τελευταία προσπέλαση: 20 Μαΐου 2024)

καθώς και η παρουσίαση των κανονιστικών πλαισίων των διασυνοριακών διαβιβάσεων δεδομένων. Χωρίζεται σε τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο θα παρουσιαστεί η προσέγγιση της Ευρωπαϊκής Ένωσης και των άλλων κρατών για την προστασία προσωπικών δεδομένων. Στο δεύτερο κεφάλαιο, θα εξεταστεί ειδικότερα το νομικό πλαίσιο των Ηνωμένων Πολιτειών Αμερικής και στο τρίτο κεφάλαιο θα αναλυθεί το «Brussels Effect», και πως η έννομη τάξη της ΕΕ επηρεάζει τις πρακτικές και την παραγωγή νομοθεσίας άλλων κρατών. Τέλος, θα παρουσιαστεί το ζήτημα των διασυνοριακών διαβιβάσεων δεδομένων, καθώς και το ρυθμιστικό πλαίσιο αυτών.

2. Η προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση και εκτός Ευρωπαϊκής Ένωσης

Σε ένα ολοένα και πιο διασυνδεδεμένο ψηφιακό τοπίο, η προστασία των προσωπικών δεδομένων έχει αναδειχθεί σε κρίσιμο ζήτημα παγκοσμίως. Η προστασία της ιδιωτικής ζωής στην Ευρώπη είναι παραδοσιακά ισχυρή για ιστορικούς, πολιτιστικούς, πολιτικούς και νομικούς λόγους (Bradford 2020, Schwartz and Peifer 2017). Στα κράτη της Ευρωπαϊκής Ένωσης, σε αντίθεση με τις προσεγγίσεις άλλων χωρών, το δικαίωμα στην ιδιωτική ζωή και στην προστασία προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα, κατοχυρωμένο από πληθώρα νομικών δεσμευτικών κειμένων. Η υιοθέτηση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων, γνωστού ως GDPR, από την Ευρωπαϊκή Ένωση αποτελεί ένα σημείο καμπής για την εξέλιξη της προστασίας δεδομένων παγκοσμίως. Σε διεθνές επίπεδο, έχουν υιοθετηθεί διαφορετικές προσεγγίσεις, με κάποιες χώρες, όπως οι Ηνωμένες Πολιτείες Αμερικής, μην έχουν ενσωματώσει στην εθνική τους έννομη τάξη ένα ολοκληρωμένο ενιαίο νομοθέτημα, ενώ άλλες, όπως η Ιαπωνία και η Βραζιλία, να έχουν θεσπίσει αντίστοιχους νόμους με τον GDPR. Στην ενότητα αυτή, θα εξεταστούν οι διαφορετικές προσεγγίσεις που έχουν υιοθετηθεί παγκοσμίως για την προστασία των προσωπικών δεδομένων.

2.1 Η νομοθετική εξέλιξη στην Ευρωπαϊκή Ένωση

2.1.1 Από την Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου στο Χάρτη Θεμελιωδών Δικαιωμάτων

Στην Ευρώπη, το δικαίωμα προστασίας της ιδιωτικής ζωής διατυπώθηκε για πρώτη φορά στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) στο άρθρο 8, που τέθηκε σε εφαρμογή το 1953. Παρά το γεγονός ότι το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν περιλαμβάνεται ρητώς στην ΕΣΔΑ, έχει καταστεί σαφές από τη νομολογία του Ευρωπαϊκού Δικαστηρίου Ανθρωπίνων Δικαιωμάτων ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να εμπίπτει στο πεδίο εφαρμογής του άρθρου 8 της ΕΣΔΑ, όταν τα δεδομένα αφορούν πτυχές της ιδιωτικής ζωής[3] (ΕΔΔΑ,). Αυτό εξαρτάται από τη

[3] Όπως επισημαίνεται στο δελτίο του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (διαθέσιμο στο: https://www.echr.coe.int/documents/d/echr/FS_Data_ENG), η απλή αποθήκευση δεδομένων που αφορούν την ιδιωτική ζωή ενός ατόμου συνιστά επέμβαση κατά την έννοια του άρθρου 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου, το οποίο κατοχυρώνει το δικαίωμα του σεβασμού της ιδιωτικής και οικογενειακής ζωής. Η μεταγενέστερη χρήση των αποθηκευμένων πληροφοριών δεν έχει καμία επίπτωση στην παραπάνω διαπίστωση. Το ΕΔΔΑ έχει κρίνει σημαντικές

φύση των δεδομένων, το πλαίσιο στο οποίο γίνεται η επεξεργασία των δεδομένων, τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα και τα αποτελέσματα της επεξεργασίας (Kramer & Hoar, 2017).

Το 1948, ιδρύθηκε ο Οργανισμός Ευρωπαϊκής Επιτροπής Οικονομικής Συνεργασίας, με σκοπό να διαχειριστεί την ανοικοδόμηση της Ευρώπης μετά τον Β' Παγκόσμιο Πόλεμο (Warren, 1998). Ο οργανισμός αυτός αργότερα επεκτάθηκε και σε μη ευρωπαϊκά κράτη και μετασχηματίστηκε στον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) με στόχο την ενίσχυση της διεθνούς συνεργασίας[4] (OECD, ND). Ο ΟΟΣΑ ενέκρινε το 1980 ένα σύνολο διεθνών κατευθυντήριων γραμμών για την προστασία της ιδιωτικής ζωής και των δεδομένων, γνωστών ως «Κατευθυντήριες γραμμές που διέπουν την προστασία της ιδιωτικής ζωής και τις διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα». Αυτές οι Κατευθυντήριες Γραμμές διατύπωσαν θεμελιώδεις αρχές για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής και αποτέλεσαν τη βάση για την μεταγενέστερη εξέλιξη της νομοθεσίας της Ευρωπαϊκής Ένωσης (Park, 2020).

Ορισμένες από τις αρχές που περιλαμβάνονται στις Κατευθυντήριες Γραμμές του ΟΟΣΑ, είναι: α) η αρχή ότι ο σκοπός της συλλογής δεδομένων πρέπει να είναι συναφής με τη χρήση τους, β) τα δεδομένα θα πρέπει να προστατεύονται από την απώλεια και τη μη εξουσιοδοτημένη πρόσβαση, γ) τα άτομα θα πρέπει να έχουν το δικαίωμα να γνωρίζουν ποια δεδομένα συλλέγονται γι' αυτά, δ) τα άτομα θα πρέπει να έχουν το δικαίωμα πρόσβασης σε όλα τα δεδομένα που το αφορούν, και ε) τα άτομα θα πρέπει να μπορούν να αντιταχθούν στη διατήρηση δεδομένων ή να τροποποιήσουν ή να διαγράψουν δεδομένα που τους αφορούν (OECD, 1980). Οι Κατευθυντήριες Γραμμές του ΟΟΣΑ αποτελούν παγκόσμιο πρότυπο για την προστασία προσωπικών δεδομένων, αλλά η ισχύς τους είναι περιορισμένη, καθώς δεν είναι νομικά δεσμευτικές για τις χώρες-μέλη του ΟΟΣΑ (Kramer & Hoar, 2017). Οι Κατευθυντήριες Γραμμές του ΟΟΣΑ για την προστασία της ιδιωτικής ζωής και τις διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα, αναθεωρήθηκαν στις 11 Ιουλίου 2013 (Cecile de Terwange, 2021).

Το 1981 υιοθετήθηκε η Σύμβαση 108 του Συμβουλίου της Ευρώπης, επίσημα γνωστή ως «Σύμβαση για την προστασία των φυσικών προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα» (εφεξής «Σύμβαση 108»), που αποτελεί ακρογωνιαίο λίθο των διεθνών προσπαθειών για την προστασία των δεδομένων. Η Σύμβαση 108 αποτέλεσε το θεμέλιο για τα καθεστώτα προστασίας δεδομένων των 46 κρατών μελών[5] του Συμβουλίου της Ευρώπης, καθώς και πολλών χωρών εκτός Ευρωπαϊκών συνόρων (Cecile de Terwange, 2021).

υποθέσεις σχετικά με την επεξεργασία προσωπικών δεδομένων, όπως η Jehovah's Witnesses v. Finland, Drelon v. France, Klass and Others v. Germany κα.

[4] Η ιστορία του ΟΟΣΑ διαθέσιμη στην επίσημη ιστοσελίδα του στο: https://www.oecd.org/about/history/oeec/ (τελευταία προσπέλαση: 21 Απριλίου 2024)

[5] Στα μέλη του Συμβουλίου της Ευρώπης περιλαμβάνονται όλα τα ευρωπαϊκά κράτη εκτός της Λευκορωσίας, του Καζακστάν, της Πόλης του Βατικανού, της Ρωσίας, που αποβλήθηκε το 2022 λόγω της εισβολής στην Ουκρανία και των ευρωπαϊκών κρατών με περιορισμένη αναγνώριση, ενώ καθεστώς παρατηρητή έχει παραχωρηθεί στις Ηνωμένες Πολιτείες Αμερικής, την Αγία Έδρα, την

Η εν λόγω Σύμβαση, που αποτελεί τη μόνη δεσμευτική διεθνή Σύμβαση για την προστασία δεδομένων προσωπικού χαρακτήρα, καθορίζει αρχές και πρότυπα για την προστασία των δεδομένων προσωπικού χαρακτήρα, με στόχο να διασφαλιστεί ο σεβασμός των δικαιωμάτων των ατόμων στην ιδιωτική ζωή στο πλαίσιο της αυτοματοποιημένης επεξεργασίας. Η Σύμβαση 108 θεσπίζει θεμελιώδεις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, μεταξύ των οποίων την αρχή του περιορισμένου σκοπού, την αρχή της ποιότητας των δεδομένων και την ύπαρξη διαφόρων δικαιωμάτων του υποκειμένου, όπως είναι το δικαίωμα πρόσβασης και το δικαίωμα διαγραφής (Cecile de Terwange, 2022).

Η Σύμβαση 108 εφαρμόζεται τόσο σε φορείς του δημόσιου, όσο και του ιδιωτικού τομέα[6] που ασχολούνται με την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη χρησιμοποιούμενη τεχνολογία[7]. Καλύπτει ένα ευρύ φάσμα δραστηριοτήτων, συμπεριλαμβανομένης της συλλογής, αποθήκευσης, ανάκτησης, διαβούλευσης, χρήσης, κοινοποίησης και διάδοσης δεδομένων προσωπικού χαρακτήρα[8]. Επιπλέον, η Σύμβαση 108 παρέχει ένα πλαίσιο για τη διεθνή συνεργασία στον τομέα της προστασίας δεδομένων, διευκολύνοντας τη διαβίβαση δεδομένων μεταξύ των κρατών που την έχουν υπογράψει, διασφαλίζοντας παράλληλα ότι υπάρχουν επαρκείς εγγυήσεις για την προστασία των δικαιωμάτων των φυσικών προσώπων στην ιδιωτική ζωή[9].

Το κείμενο της Σύμβασης 108, συντάχθηκε σε μία εποχή που δεν υπήρχαν το Διαδίκτυο, τα κοινωνικά δίκτυα, τα μεγάλα δεδομένα ή ο γεωεντοπισμός. Ως εκ τούτου, η Σύμβαση δεν κατέστη επαρκής ώστε να δώσει ικανοποιητικές λύσεις στις νέες προκλήσεις που προέκυψαν στο σημερινό κόσμο. Τις επόμενες δεκαετίες, η Σύμβαση 108 εκσυγχρονίστηκε, με τις κυριότερες αλλαγές να αφορούν την πρόβλεψη των γενετικών και βιομετρικών δεδομένων[10], την προσθήκη της αρχής της διαφάνειας της επεξεργασίας[11] και την διαβίβαση προσωπικών δεδομένων σε κράτη που δεν αποτελούν μέλη της σύμβασης[12] (Cecile de Terwange, 2021). Η «Εκσυγχρονισμένη» Σύμβαση 108 γνωστή και ως «Σύμβαση 108+», οριστικοποιήθηκε το 2018 και έχει υπογραφεί μέχρι σήμερα από περισσότερα από 40 κράτη[13] (Greenleaf, 2018).

Το 2009, τέθηκε σε εφαρμογή ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, όπου στο άρθρο 8 κατοχυρώνεται το δικαίωμα στην προστασία των δεδομένων

Ιαπωνία, τον Καναδάς και το Μεξικό, https://www.coe.int/el/web/about-us/our-member-states (τελευταία προσπέλαση: 18 Απριλίου 2024)

[6] Σύμβαση 108, άρθρο 3 παρ. 1

[7] Σύμβαση 108, άρθρο 2 (β)

[8] Σύμβαση 108, άρθρο 2 (γ)

[9] Σύμβαση 108, άρθρα 12-17

[10] Σύμβαση 108+, άρθρο 6 παρ. 1

[11] Σύμβαση 108+, άρθρο 8

[12] Σύμβαση 108+, άρθρο 14

[13] Μέχρι σήμερα (21.04.2024) έχουν υπογράψει τη Σύμβαση 108 55 κράτη, μεταξύ των οποίων το Μεξικό, η Τυνησία, το Μαρόκο και άλλες, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108, (τελευταία προσπέλαση: 21 Απριλίου 2024), ενώ το Πρωτόκολλο έχει υπογραφεί από περισσότερες από 40 χώρες παγκοσμίως, https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet, (τελευταία προσπέλαση: 21 Απριλίου 2024)

προσωπικού χαρακτήρα, αναγνωρίζοντάς το ως θεμελιώδες ανθρώπινο δικαίωμα στην Ευρωπαϊκή Ένωση (ΕΕ). Η διάταξη αυτή έχει σημαντικές συνέπειες για τις προσπάθειες προστασίας των δεδομένων στην Ευρωπαϊκή Ένωση. Το άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων (ΧΘΔ) υπογραμμίζει τη δέσμευση της ΕΕ για την προστασία των δικαιωμάτων των ατόμων και την προώθηση υπεύθυνων πρακτικών επεξεργασίας δεδομένων. Αξιοσημείωτο είναι ότι σε αντίθεση με την ΕΣΔΑ, στο Χάρτη Θεμελιωδών Δικαιωμάτων, διακρίνεται το δικαίωμα της ιδιωτικής ζωής (Άρθρο 7) από το δικαίωμα της προστασίας των προσωπικών δεδομένων (Άρθρο 8), καθιστώντας ο ευρωπαϊκός νομοθέτης σαφή την πρόθεση του να διαφυλάξει την προστασία των προσωπικών δεδομένων ως ξεχωριστό θεμελιώδες δικαίωμα (Mostert, 2018).

2.1.2 Η Οδηγία 95/46/ΕΚ

Το 1995, η Ευρωπαϊκή Ένωση εξέδωσε την Οδηγία για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Οδηγία 95/46/ΕΚ).

Η Οδηγία απαιτούσε από τα 28 Κράτη Μέλη να θεσπίσουν εθνικές νομοθεσίες που προστατεύουν τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων, και ιδίως το δικαίωμά τους στην ιδιωτική ζωή όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η Οδηγία επιτάσσει την διαφύλαξη από όλα τα κράτη μέλη ότι όλες οι προσωπικές πληροφορίες προστατεύονται με επαρκή ασφάλεια και ότι τα υποκείμενα των δεδομένων έχουν το δικαίωμα να λαμβάνουν αντίγραφα των πληροφοριών που συλλέγονται, καθώς και το δικαίωμα διόρθωσης ή διαγραφής των προσωπικών τους δεδομένων[14]. Σύμφωνα με την Οδηγία, η επεξεργασία δεδομένων θεωρούνταν νόμιμη εφόσον ο υπεύθυνος επεξεργασίας είχε λάβει τη συγκατάθεση των υποκειμένων των δεδομένων πριν από τη σύναψη της άδειας χρήσης, ή η επεξεργασία ήταν απαραίτητη για την εκτέλεση σύμβασης, ή για την τήρηση υποχρέωσης εκ του νόμου, ή για την εκπλήρωση έργου δημοσίου συμφέροντος ή για την επίτευξη εννόμου συμφέροντος τρίτου[15].

Υπό το καθεστώς της Οδηγίας, οι εταιρείες που είτε ήταν εγκατεστημένες στην ΕΕ, είτε δεν είχαν εγκατάσταση στην ΕΕ, αλλά για τους σκοπούς επεξεργασίας δεδομένων προσωπικού χαρακτήρα προσέφευγαν σε μέσα, αυτοματοποιημένα ή όχι, ευρισκόμενα στο έδαφος κράτους μέλους της ΕΕ, έπρεπε να συμμορφώνονται με την Οδηγία. Επιπροσθέτως, μια εταιρεία δεν μπορούσε να διαβιβάζει δεδομένα σε άλλες χώρες, χωρίς να υπάρχει «επαρκές επίπεδο» προστασίας δεδομένων αντίστοιχο με αυτό της ΕΕ[16]. Τέλος, σύμφωνα με την Οδηγία, μια εταιρεία υποχρεούνταν να λαμβάνει ρητή συγκατάθεση από τα υποκείμενα των δεδομένων ως προς τη συλλογή δεδομένων σχετικά με τη φυλή, την εθνικότητα, τα πολιτικά φρονήματα, τη συμμετοχή σε συνδικάτα, τη σωματική και ψυχική υγεία, τις σεξουαλικές προτιμήσεις και το ποινικό μητρώο, που θεωρούνται ευαίσθητα προσωπικά δεδομένα[17].

[14] Οδηγία 95/46/ΕΚ, άρθρο 12 (και αιτιολογική σκέψη 41)
[15] Οδηγία 95/46/ΕΚ, άρθρο 7, (και αιτιολογική σκέψη 40)
[16] Οδηγία 95/46/ΕΚ, άρθρο 25
[17] Οδηγία 95/46/ΕΚ, άρθρο 8

Το βασικότερο μειονέκτημα της Οδηγίας του 1995 ήταν ότι άφηνε περιθώριο διαφορετικής ερμηνείας και εφαρμογής των διατάξεών της μεταξύ των επιμέρους κρατών-μελών. Επιπλέον, το ταχέως εξελισσόμενο τοπίο στην αποθήκευση, συλλογή και διαβίβαση δεδομένων επέβαλε μια επικαιροποίηση του ρυθμιστικού περιβάλλοντος της ΕΕ (Park, 2020). Οι τεχνολογικές εξελίξεις στον κυβερνοχώρο κατέστησαν σαφές ότι η Οδηγία του 1995, που υιοθετήθηκε όταν το Facebook και το Instagram δεν είχαν ακόμη εφευρεθεί, δεν παρείχαν τα απαραίτητα εχέγγυα για την προστασία των προσωπικών δεδομένων στη σύγχρονη ψηφιακή κοινωνία.

2.1.3 Ο Γενικός Κανονισμός για την Προστασία Δεδομένων

Η Ευρωπαϊκή Επιτροπή αντικατέστησε την Οδηγία του 1995 με τον Γενικό Κανονισμό Προστασίας Δεδομένων, με ισχύ από τις 25 Μαΐου 2018. Αρχικώς, τον Ιανουάριο του 2012 η Επιτροπή πρότεινε μια επικαιροποίηση της υφιστάμενης νομοθεσίας για την προστασία των δεδομένων ώστε να καταστεί η Ευρωπαϊκή Ένωση κατάλληλη για την ψηφιακή εποχή. Ο GDPR εγκρίθηκε στις 14 Απριλίου 2016 και είχε ως στόχο να ενισχύσει, να ενοποιήσει, και να καταστήσει πιο συνεκτικούς τους νόμους για την προστασία των δεδομένων και το πλαίσιό του σε όλα τα κράτη της Ευρωπαϊκής Ένωσης.

Ο GDPR αποτελεί τον ακρογωνιαίο λίθο της ευρωπαϊκής -και όχι μόνο- νομοθεσίας για την προστασία της ιδιωτικής ζωής και θεωρείται το πιο ολοκληρωμένο παγκοσμίως καθεστώς προστασίας της ιδιωτικής ζωής. Καθιερώνει κοινούς κανόνες για την επεξεργασία δεδομένων σε όλη την Ευρωπαϊκή Ένωση και είναι άμεσα δεσμευτικός για τα υποκείμενα που βρίσκονται στην ΕΕ και εκτός συνόρων αυτής (Peukert et al, 2022). Η Επιτροπή επεδίωξε να διορθώσει τη στρέβλωση του ανταγωνισμού μεταξύ των κρατών λόγω άνισης νομοθεσίας για την προστασία των δεδομένων και να ενισχύσει την παρακολούθηση και την επιβολή, ώστε περισσότερες εταιρείες και οργανισμοί να συμμορφωθούν με τους νόμους της ΕΕ (Park, 2020).

Μόλις τέθηκε σε ισχύ ο GDPR, η Οδηγία του 1995 καταργήθηκε και όλα τα κράτη μέλη και τα υποκείμενα αυτών όφειλαν να συμμορφωθούν με το νέο Κανονισμό για τα δεδομένα. Σε αντίθεση με την Οδηγία, ο GDPR είναι ένα δεσμευτικό νομοθέτημα, που ισχύει αυτόματα σε όλα τα κράτη μέλη της ΕΕ χωρίς την ανάγκη ενσωμάτωσης των κανόνων του στην εθνική νομοθεσία κάθε κράτους μέλους της ΕΕ. Ο GDPR θεμελίωσε σημαντικές αρχές, όπως αυτή της διαφάνειας, της νομιμότητας, της δικαιοσύνης και της ελαχιστοποίησης δεδομένων, ενώ αναγνώρισε διευρυμένα δικαιώματα στα υποκείμενα και αντίστοιχα αυστηρές υποχρεώσεις στις επιχειρήσεις που διενεργούν την επεξεργασία (Park, 2020).

Ο GDPR αποκλίνει σημαντικά από την Οδηγία του 1995 σε βασικά σημεία. Πρώτον, ο GDPR θέτει αυστηρότερα κριτήρια για την απόκτηση δεδομένων προσωπικού χαρακτήρα από ό,τι επιτρεπόταν προηγουμένως, απαιτώντας ρητή και ενημερωμένη συγκατάθεση από τους χρήστες[18]. Δεύτερον, οι κυρώσεις είναι αυστηρότερες ώστε να διασφαλίζεται ότι οι εταιρείες και οι οργανισμοί συμμορφώνονται με τα νέα μέτρα[19]. Τρίτον, τα δικαιώματα των

[18] GDPR, άρθρο 6
[19] GDPR, άρθρο 83

υποκειμένων των δεδομένων επεκτείνονται ώστε να δοθεί στους πολίτες της ΕΕ μεγαλύτερος έλεγχος των προσωπικών τους δεδομένων[20] (Park, 2020).

Τέλος, το πεδίο εφαρμογής του νέου Κανονισμού είναι ευρύτερο σε σχέση με την Οδηγία και εισάγει την αρχή της εξωεδαφικότητας, δηλαδή την εφαρμογή του GDPR και εκτός των συνόρων της ΕΕ. Ο GDPR εφαρμόζεται σε όλες τις αμερικανικές και ξένες επιχειρηματικές οντότητες που είτε (α) προσφέρουν αγαθά ή υπηρεσίες σε οποιαδήποτε από τις τριάντα χώρες του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ) είτε (β) παρακολουθούν τις δραστηριότητες των δεδομένων υποκειμένων δεδομένων εντός της ΕΕ[21]. Η διεύρυνση του πεδίου εφαρμογής της νομοθεσίας της ΕΕ, δικαιολογείται με το σκεπτικό ότι η τεχνολογική πρόοδος έχει οδηγήσει στην επεξεργασία των προσωπικών δεδομένων των κατοίκων της ΕΕ εκτός των συνόρων της σε πρωτόγνωρη κλίμακα (Rustad & Koenig, 2019).

2.2 Οι διεθνείς προσεγγίσεις

2.2.1 Ηνωμένες Πολιτείες

Οι Ηνωμένες Πολιτείες Αμερικής έχουν υιοθετήσει μία διαφορετική προσέγγιση σε σχέση με την Ευρωπαϊκή Ένωση. Οι ΗΠΑ δεν διαθέτουν έναν ολοκληρωμένο ομοσπονδιακό νόμο για την προστασία των δεδομένων, παρόμοιο με τον GDPR. Αντιθέτως, η προστασία των δεδομένων διέπεται από ένα συνονθύλευμα διαφορετικών νόμων για κάθε τομέα, όπως ο Health Insurance Portability and Accountability Act (HIPAA) για τα δεδομένα υγειονομικής περίθαλψης και ο Gramm-Leach-Bliley Act (GLBA) για τα χρηματοοικονομικά δεδομένα. Επιπλέον, οι ΗΠΑ βασίζονται σε μεγάλο βαθμό στην αυτορρύθμιση και στα πρότυπα του κλάδου, με φορείς όπως η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) να επιβάλλουν την προστασία της ιδιωτικής ζωής μέσω των αποφάσεων της (Rustad & Koenig, 2019).

Εξάλλου, κάποιες Πολιτείες των ΗΠΑ έχουν ακολουθήσει το πρότυπο της ΕΕ και έχουν υιοθετήσει αντίστοιχες νομοθεσίες στον τομέα των προσωπικών δεδομένων. Ειδικότερα, το 2018 στην Πολιτεία της Καλιφόρνια ψηφίστηκε ο California Consumer Privacy Act of 2018 («CCPA»). Ο νόμος αυτός, που τέθηκε σε ισχύ το 2020, ακολουθεί σε μεγάλο ποσοστό το πρότυπο του GDPR και αποτελεί την πιο αξιοσημείωτη πολιτειακή νομοθεσία για την προστασία της ιδιωτικής ζωής των δεδομένων στις ΗΠΑ. Λίγο μετά την ψήφιση του CCPA από την Καλιφόρνια, η Νέα Υόρκη θέσπισε επίσης έναν ολοκληρωμένο νόμο για την προστασία της ιδιωτικής ζωής των δεδομένων, το Stop Hacks and Electronic Data Security Act («SHIELD Act»), ακολουθώντας τον GDPR. Ο νόμος SHIELD Act αντιμετωπίζει θέματα προστασίας της ιδιωτικής ζωής των δεδομένων που τονίζονται στον GDPR, αλλά διαφέρει ως προς την προσέγγισή του για τα χρηματοπιστωτικά ιδρύματα. Παράλληλα με την Καλιφόρνια και τη Νέα Υόρκη , πολλές άλλες πολιτείες έχουν εισαγάγει νομοθεσίες που ενσωματώνουν σημαντικές διατάξεις του GDPR της ΕΕ (Field E., 2020).

2.2.2 Ιαπωνία

Στην Ιαπωνία η προστασία των προσωπικών δεδομένων επιτυγχάνεται μέσω του Act on the Protection of Personal Information («APPI») που εφαρμόζεται τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, και η αρμοδιότητα της εποπτείας της εφαρμογής του νόμου αυτού έχει

[20] GDPR, άρθρα 16-22

[21] GDPR, άρθρο 3

απονεμηθεί στην Επιτροπή για την Προστασία Προσωπικών Πληροφοριών (Personal Information Protection Commission – «PPC»). Ο APPI, ψηφίστηκε αρχικά το 2003, αλλά από το 2015 και μετά επήλθαν εκτεταμένες τροποποιήσεις αναφορικά με τα ευαίσθητα δεδομένα, τα μεγάλα δεδομένα και τις ενισχυμένες εξουσίες επιβολής για την ιαπωνική αρχή προστασίας δεδομένων (Miyashita, 2020).

Ο τροποποιημένος APPI περιλαμβάνει, μεταξύ άλλων, προστασία για τις διασυνοριακές διαβιβάσεις δεδομένων προσωπικού χαρακτήρα από την Ιαπωνία. Ειδικότερα, ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να διαβιβάζονται σε αλλοδαπή χώρα εκτός εάν: α) το υποκείμενο των δεδομένων έχει δώσει συγκεκριμένη εκ των προτέρων συγκατάθεση για τη διαβίβαση, β) η χώρα στην οποία είναι εγκατεστημένος ο παραλήπτης, διαθέτει νομικό σύστημα που θεωρείται ισοδύναμο ως προς την προστασία της ιδιωτικής ζωής με το ιαπωνικό σύστημα, ή γ) ο παραλήπτης αναλαμβάνει την υποχρέωση να λάβει επαρκή προληπτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα που καθορίζονται από την Επιτροπή για την Προστασία Προσωπικών Πληροφοριών (Schwartz, 2019).

Ο APPI, περιλαμβάνει τις βασικές αρχές των Κατευθυντήριων Γραμμών του ΟΟΣΑ και περιέχει αρκετές αντίστοιχες διατάξεις με τον GDPR. Γενικώς, η Ιαπωνία, μετά την εισαγωγή των σημαντικών τροποποιήσεων του APPI, θεωρείται μία χώρα με ολοκληρωμένο και σαφές νομικό πλαίσιο για την προστασία προσωπικών δεδομένων, δεδομένου και του καθοριστικού ρόλου που έχει η PPC για την εποπτεία της εφαρμογή του APPI και την έκδοση ερμηνευτικών κατευθυντήριων γραμμών.

2.2.3 Κίνα

Η Κίνα αρχικώς είχε υιοθετήσει αντίστοιχη προσέγγιση με αυτή των Ηνωμένων Πολιτειών όσον αφορά την προστασία της ιδιωτικής ζωής των δεδομένων. Έτσι, δεν υπήρχε ένα ενιαίο ολοκληρωμένο νομοθέτημα, αλλά αντίθετα η προστασία των προσωπικών δεδομένων παρεχόταν από διάφορους νόμους που δεν σχετίζονταν ακριβώς με τη συλλογή και την επεξεργασία δεδομένων. Οι κανόνες της Κίνας για την προστασία των προσωπικών δεδομένων ήταν διάσπαρτοι σε περισσότερους από 30 ειδικούς νόμους και διοικητικούς κανονισμούς, ενώ το δικαίωμα στην προστασία των προσωπικών δεδομένων, δεν προβλεπόταν στο Σύνταγμα της Κίνας μέχρι την ψήφιση του Συντάγματος του 1982 (Hornuf, Mangold & Yang, 2023).

Η προστασία των προσωπικών δεδομένων βασιζόταν σε νόμους όπως οι Γενικές Αρχές του Αστικού Δικαίου του 1986, ο Ποινικός Νόμος, το άρθρο 252 του νόμου περί Αδικοπρακτικής Ευθύνης του 2010, ο νόμος περί Τηλεπικοινωνιών και Προσωπικών Δεδομένων χρηστών του διαδικτύου του 2013, και ο νόμος για την Κυβερνοασφάλεια (Cybersecurity Law of China - CSL) του 2016 για την παροχή προστασίας των προσωπικών δεδομένων, ο οποίος αποτέλεσε το πρώτο σημαντικό βήμα προς έναν ολοκληρωμένο νόμο για την προστασία των δεδομένων. Ο CSL ήταν ένα πολύ ευρύ σύνολο ρυθμίσεων και ίσχυε μόνο για εταιρείες που βρίσκονται εντός της Κίνας (Kelly, 2022).

Το 2021 τέθηκε σε εφαρμογή στην Κίνα ο νόμος για την Προστασία Προσωπικών Πληροφοριών (Personal Information Protection Law - PIPL), ο πρώτος ολοκληρωμένος και σαφής νόμος για την προστασία των ιδιωτικών πληροφοριών των φυσικών προσώπων. Ο

PIPL εφαρμόζεται σε κάθε επιχείρηση εντός της χώρας ή εκτός της Κίνας που χειρίζεται οποιαδήποτε προσωπική πληροφορία οποιουδήποτε φυσικού προσώπου εντός της χώρας. Ο PIPL διαμορφώθηκε σε μεγάλο βαθμό σύμφωνα με τον GDPR, και παρέχει διάφορα δικαιώματα στους πολίτες που προστατεύονται βάσει του κανονισμού. Τα δικαιώματα αυτά περιλαμβάνουν το δικαίωμα πρόσβασης, το δικαίωμα διόρθωσης, το δικαίωμα διαγραφής, το δικαίωμα ανάκλησης της συγκατάθεσης, το δικαίωμα ακύρωσης ενός λογαριασμού, το δικαίωμα λήψης αντιγράφων και το δικαίωμα υποβολής καταγγελίας σε περιπτώσεις όπου η αυτοματοποιημένη λήψη αποφάσεων είχε σημαντικό αντίκτυπο στα δικαιώματα των υποκειμένων (Amdahl, 2023).

Την ίδια χρονιά με το νόμο PIPL, τέθηκε σε εφαρμογή και ο νόμος της Κίνας για την Ασφάλεια των Δεδομένων (Data Security Law – DSL), που αποτελεί τον τρίτο σημαντικό νόμο για την προστασία δεδομένων μαζί με τον PIPL και τον CSL. Ο DSL, εφαρμόζεται και σε μη προσωπικά δεδομένα και περιέχει διατάξεις σχετικά με την ασφάλεια και την προστασία των δεδομένων (Hornuf, Mangold & Yang, 2023).

Συνοψίζοντας, παρά το γεγονός ότι δεν υπάρχει ένα ενιαίο ολοκληρωμένο νομοθέτημα για την προστασία προσωπικών πληροφοριών, ο βασικός νόμος είναι ο PIPL, που σε μεγάλο βαθμό προσεγγίζει τις διατάξεις του GDPR και θεωρείται ότι εγγυάται σε ικανοποιητικό βαθμό την προστασία προσωπικών δεδομένων στα φυσικά πρόσωπα της χώρας (Hornuf, Mangold, Yang, 2023).

2.2.4 Καναδάς

Το καθεστώς προστασίας δεδομένων του Καναδά διέπεται κυρίως από τον Personal Information Protection and Electronic Documents Act (PIPEDA), ο οποίος τέθηκε σε εφαρμογή το 2001. Ο PIPEDA ρυθμίζει τη συλλογή, τη χρήση και τη γνωστοποίηση προσωπικών πληροφοριών καταναλωτών και εργαζομένων από οργανισμούς του ιδιωτικού τομέα που ασκούν εμπορικές δραστηριότητες (Jaar & Zeller, 2009).

Υπό το καθεστώς του PIPEDA, παρέχεται στα υποκείμενα ένα ευρύ φάσμα δικαιωμάτων, μεταξύ των οποίων, το δικαίωμα υποβολής παραπόνων απευθείας στην επιχείρηση και μετέπειτα στην αρμόδια αρχή, το δικαίωμα πρόσβασης και το δικαίωμα ελαχιστοποίησης δεδομένων (Jaar & Zeller, 2009). Το Γραφείο του Επιτρόπου Προστασίας Προσωπικών Δεδομένων του Καναδά (Office of the Privacy Commissioner of Canada - OPC) επιβλέπει τη συμμόρφωση με τον PIPEDA και διερευνά καταγγελίες που σχετίζονται με παραβιάσεις της ιδιωτικής ζωής (Feys, 2022).

Εκτός από το βασικό ομοσπονδιακό νόμο, ορισμένες επαρχίες, όπως η Βρετανική Κολομβία και το Κεμπέκ, έχουν θεσπίσει τη δική τους νομοθεσία για την προστασία της ιδιωτικής ζωής. Συνεπώς, ο Καναδάς, παρά το γεγονός ότι έχει έναν ενιαίο νόμο για την προστασία προσωπικών δεδομένων σε ομοσπονδιακό επίπεδο, διαθέτει ένα πολύπλοκο ρυθμιστικό πεδίο στον τομέα αυτό, λόγω της ύπαρξης πληθώρας σχετικών επαρχιακών νομοθεσιών (Jaar, Zeller, 2009).

2.2.5 Βραζιλία

Η Βραζιλία έχει υιοθετήσει ολοκληρωμένο νομικό καθεστώς για την προστασία δεδομένων, μετά την ψήφιση του General Data Protection Law (LGPD), ο οποίος είναι σε ισχύ από το 2020. Πριν από τη θέσπιση του LGPD, η νομοθεσία για την προστασία της ιδιωτικής ζωής στη

Βραζιλία αποτελούνταν από διάφορες διάσπαρτες διατάξεις. Για παράδειγμα, ο Νόμος 12.965/2014 και το Κανονιστικό Διάταγμα αριθ. 8.771/16 (Νόμος της Βραζιλίας για το Διαδίκτυο) επέβαλαν απαιτήσεις σχετικά με την ασφάλεια και την επεξεργασία δεδομένων προσωπικού χαρακτήρα και άλλες υποχρεώσεις για τους παρόχους υπηρεσιών και παρείχαν δικαιώματα για τους χρήστες του Διαδικτύου (Jonatas de Souza et al, 2020).

Σε αντιστοιχία με τον GDPR, ο LGPD αποσκοπεί στην προστασία των δικαιωμάτων των ατόμων στην ιδιωτική ζωή και στη ρύθμιση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από φορείς του δημόσιου και του ιδιωτικού τομέα. Ο LGPD θεσπίζει αρχές για την επεξεργασία δεδομένων, συμπεριλαμβανομένης της διαφάνειας, του περιορισμού του σκοπού και της ελαχιστοποίησης των δεδομένων, και παρέχει στα άτομα δικαιώματα όπως η πρόσβαση, η διόρθωση και η διαγραφή των προσωπικών τους δεδομένων. Περιλαμβάνει επίσης διατάξεις για τη διασυνοριακή διαβίβαση δεδομένων, απαιτώντας από τους υπεύθυνους επεξεργασίας δεδομένων να διασφαλίζουν επαρκείς εγγυήσεις για τη διεθνή διαβίβαση δεδομένων, όπως μέσω τυποποιημένων συμβατικών ρητρών ή συμφωνιών προστασίας δεδομένων (Jonatas de Souza et al, 2020). Η υιοθέτηση της LGPD από τη Βραζιλία αντικατοπτρίζει τη δέσμευσή της να ευθυγραμμιστεί με τα διεθνή πρότυπα προστασίας δεδομένων και να προωθήσει μια κουλτούρα συμμόρφωσης της ιδιωτικής ζωής μεταξύ των οργανισμών (Jonatas de Souza et al, 2020).

2.2.6 Αυστραλία

Στην Αυστραλία, ισχύει σε ομοσπονδιακό επίπεδο ο Privacy Act 1988, που αποτελεί το βασικό πυλώνα της προστασίας δεδομένων των φυσικών προσώπων στη χώρα. Ο νόμος αυτός, που τροποποιήθηκε σημαντικά το 2012, ρυθμίζει την επεξεργασία των προσωπικών δεδομένων από τις μεγάλες επιχειρήσεις και απαιτεί από τους οργανισμούς του ιδιωτικού τομέα να συμμορφώνονται με τις αρχές για τη συλλογή, τη χρήση, την αποκάλυψη και την επεξεργασία των προσωπικών πληροφοριών (Chaudhury & Choe, 2023).

Παράλληλα με τον Privacy Act, εφαρμόζονται και οι Australian Privacy Principles (APPs), που θέτουν ένα γενικό πλέγμα υποχρεώσεων στις επιχειρήσεις αναφορικά με την προστασία των δεδομένων των καταναλωτών από την απώλεια, την παρέμβαση ή την κατάχρηση από μη εξουσιοδοτημένα μέρη. Παρέχουν κατευθυντήριες γραμμές για τη συλλογή, την ανωνυμοποίηση, την ασφάλεια και την πώληση προσωπικών δεδομένων (Chaudhury & Choe, 2023). Η Επιτροπή Πληροφοριών (Information Commissioner) της Αυστραλίας έχει την εξουσία να διεξάγει έρευνες για την επιβολή του Privacy Act και να επιβάλλει κυρώσεις για παραβιάσεις των APPs (Watts & Casanovas 2017).

Επιπροσθέτως, οι περισσότερες Πολιτείες της Αυστραλίας, με εξαίρεση τη Δυτική και τη Νότια Αυστραλία, έχουν υιοθετήσει τη δική τους νομοθεσία για την προστασία των δεδομένων, όπως η Επικράτεια της Αυστραλιανής Πρωτεύουσας που εφαρμόζει τον Information Privacy Act 2014 και η Νέα Νότια Ουαλία που εφαρμόζει τον Privacy and Personal Information Protection Act 1998 (Watts & Casanovas, 2017).

Η ισχύουσα νομοθεσία της Αυστραλίας, που είναι κυρίως βασισμένη στις Κατευθυντήριες Γραμμές του ΟΟΣΑ, παρέχει επαρκές επίπεδο προστασίας προσωπικών δεδομένων, ωστόσο εισάγει σημαντικές εξαιρέσεις από την εφαρμογή του νόμου, όπως την επεξεργασία των δεδομένων από μικρές επιχειρήσεις και την επεξεργασία των δεδομένων

των εργαζομένων. Επιπλέον, η ύπαρξη διαφόρων νομοθεσιών τόσο σε ομοσπονδιακό επίπεδο, όσο και σε επίπεδο Πολιτειών, καθιστά το σύστημα για την προστασία δεδομένων της Αυστραλίας πολύπλοκο και ανομοιόμορφο (Watts & Casanovas 2017).

2.2.7 Ισραήλ

Στο Ισραήλ, η προστασία των δεδομένων διέπεται κυρίως από τον Protection of Privacy Law (PPL), τους Κανονισμούς για την Ασφάλεια των Δεδομένων (Data Security Regulations), καθώς και από ειδικούς κανονισμούς, όπως οι Κανονισμοί για την Προστασία της Ιδιωτικής ζωής «Μεταφορά πληροφοριών σε Βάσεις Δεδομένων εκτός των Ορίων του Κράτους», 5761-2001 (Privacy Regulations «Transfer of Data to Databases Abroad», 5761-2001), (Haber, 2020 & Gidron, 2012).

Το δικαίωμα στην ιδιωτική ζωή στο Ισραήλ προστατεύεται ως θεμελιώδες δικαίωμα σε συνταγματικό επίπεδο, σύμφωνα με τον Βασικό Νόμο 5752-1992 (Basic Law: Human Dignity and Liberty, 5752-1992). Ο βασικός νόμος για την προστασία προσωπικών δεδομένων του Ισραήλ, που είναι ο PPL, ρυθμίζει στο πρώτο μέρος του την προστασία της ιδιωτικής ζωής και στο δεύτερο μέρος την προστασία των ατόμων από την επεξεργασία των προσωπικών τους δεδομένων. Σύμφωνα με τον PPL, οι ιδιοκτήτες των βάσεων δεδομένων οφείλουν να τηρούν διάφορες απαιτήσεις, όπως την απαίτηση του περιορισμού του σκοπού, της εμπιστευτικότητα και της διαφάνειας. Στα υποκείμενα των δεδομένων παρέχονται σημαντικά δικαιώματα, όπως το δικαίωμα ελέγχου και τροποποίησης πληροφοριών. (Haber, 2020) Η Αρχή της Προστασίας της Ιδιωτικότητας του Ισραήλ (PPA), εκδίδει λεπτομερείς μη δεσμευτικές κατευθυντήριες γραμμές και εκθέσεις, ενώ ταυτόχρονα παρακολουθεί τις κοινοποιήσεις επεξεργασίας δεδομένων (Haber, 2020).

2.2.8 Νότια Αφρική

Στη Νότια Αφρική, η προστασία προσωπικών δεδομένων επιτυγχάνεται μέσω του Protection of Personal Information Act 4 (POPIA) του 2013, που τέθηκε σε εφαρμογή το 2020 (Swales, 2021). Αξιοσημείωτο είναι, ότι το δικαίωμα στην ιδιωτική ζωή αναγνωρίζεται ως θεμελιώδες ανθρώπινο δικαίωμα στο Σύνταγμα της Δημοκρατίας της Νότιας Αφρικής του 1996 (Bill of Rights of the Constitution of the Republic of South Africa 1996), (Roos, 2016).

Ο POPIA αποτελεί τον πρώτο ολοκληρωμένο και σαφή νόμο της χώρας και βασίστηκε κυρίως στις διατάξεις της Οδηγίας 95/46/ΕΚ. Ο νόμος αυτός εφαρμόζεται στον ιδιωτικό και δημόσιο τομέα για την προστασία από την επεξεργασία των προσωπικών δεδομένων όχι μόνο φυσικών προσώπων, αλλά και νομικών οντοτήτων (Swales, 2021). Επιπροσθέτως, ο POPIA θέτει ορισμένα κριτήρια για την διασυνοριακή διαβίβαση δεδομένων, η οποία επιτρέπεται εάν υφίστανται δεσμευτικοί εταιρικοί κανόνες, εάν έχει δοθεί συγκατάθεση από το υποκείμενο, εάν καθίσταται απαραίτητη για τη σύναψη σύμβασης ή για το συμφέρον του υποκειμένου (Swales, 2021).

Συμπερασματικά, ενώ οι χώρες εκτός Ευρωπαϊκής Ένωσης έχουν αναπτύξει διαφορετικές προσεγγίσεις για την προστασία των δεδομένων, υπάρχουν αρκετές χώρες οι οποίες έχουν υιοθετήσει ολοκληρωμένα ρυθμιστικά καθεστώτα για το ζήτημα αυτό, με χαρακτηριστική εξαίρεση τις Ηνωμένες Πολιτείες Αμερικής.

3. Η προστασία των προσωπικών δεδομένων στις Ηνωμένες Πολιτείες

Οι Ηνωμένες Πολιτείες Αμερικής έχουν υιοθετήσει διαφορετική προσέγγιση στην προστασία των προσωπικών δεδομένων σε σχέση με την Ευρωπαϊκή Ένωση. Το ισχύον καθεστώς των ΗΠΑ αποτελείται από ένα συνονθύλευμα διατάξεων από διαφορετικές νομοθεσίες, σε ομοσπονδιακό και πολιτειακό επίπεδο, που έχουν στόχο την προστασία των καταναλωτών από την επεξεργασία των δεδομένων. Αξιοσημείωτο παράδειγμα αποτελεί ο Νόμος της Καλιφόρνια, γνωστός ως CCPA, ο οποίος παρουσιάζει αρκετές ομοιότητες με τον GDPR, αλλά και ορισμένες διαφοροποιήσεις.

3.1 Η νομοθετική εξέλιξη

3.1.1 Η προσέγγιση των Η.Π.Α

Η προσέγγιση των Ηνωμένων Πολιτειών αναφορικά με την προστασία των προσωπικών δεδομένων διαφέρει σημαντικά σε σχέση με την προσέγγιση της Ευρωπαϊκής Ένωσης. Αρχικά, το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν προβλέπεται στο Αμερικάνικο Σύνταγμα (Renate de Bruin, 2022). Το αρχικό κείμενο του Συντάγματος των ΗΠΑ όχι μόνο δεν προέβλεπε το δικαίωμα την προστασία των δεδομένων, αλλά δεν υπήρχε αναφορά ούτε για το δικαίωμα στην ιδιωτική ζωή. Ωστόσο, η Τέταρτη Τροποποίηση λίγα χρόνια αργότερα, αποτέλεσε το θεμέλιο του δικαιώματος στην ιδιωτική ζωή. Η Τέταρτη Τροποποίηση προβλέπει ότι «Το δικαίωμα των πολιτών στην ατομική ασφάλεια, στην ασφάλεια των οικιών τους, των εγγράφων τους και των αντικειμένων τους έναντι παράλογων ερευνών και κατασχέσεων δεν θα παραβιαστεί και δεν θα εκδοθούν εντάλματα, υπό την επιφύλαξη σοβαρής αιτίας, συνοδευόμενα από όρκο (ένορκη καταγγελία) ή επιβεβαίωση (αποδείξεις), και ειδική περιγραφή του τόπου που θα ερευνηθεί και των ατόμων ή των αντικειμένων που θα συλληφθούν.». Παρόλο που η Τέταρτη Τροποποίηση δεν παρέχει καμία πρόβλεψη για την προστασία της ιδιωτικής ζωής έναντι της συλλογής και χρήσης προσωπικών δεδομένων από ιδιώτες, το δικαίωμα αυτό έχει αναγνωριστεί από τα δικαστήρια και έναντι ιδιωτικών φορέων (Calia, 2022).

Εξάλλου, η προστασία των προσωπικών δεδομένων έχει θεμελιωθεί και σε άλλα συνταγματικά δικαιώματα (Huie, Laribee, Hogan, 2002 & Solove, Schwartz, 2022). Πιο συγκεκριμένα, η συνταγματική προστασία της ιδιωτικής ζωής στις ΗΠΑ βασίζεται κυρίως στην Πρώτη Τροπολογία (προστασία της ελευθερίας του λόγου και της ελευθερίας του συνέρχεσθαι) και την Πέμπτη Τροπολογία (προνόμιο κατά της αυτοενοχοποίησης), (Tzanou, 2020).

Η αμερικανική προσέγγιση για την προστασία της ιδιωτικής ζωής και των δεδομένων συνίσταται σε ένα συνονθύλευμα πολιτειακών και ομοσπονδιακών νόμων, ενώ δεν υπάρχει ένα ολοκληρωμένο γενικό πλαίσιο. Σε ομοσπονδιακό επίπεδο δεν υπάρχει ένα ενιαίο νομοθέτημα, αλλά διάσπαρτοι νόμοι σε διάφορους τομείς, με ρυθμίσεις που αποκλίνουν μεταξύ τους (Calia, 2022). Επιπροσθέτως, δεν υπάρχει ενιαία αρμόδια αρχή επιφορτισμένη με την επιβολή της προστασίας των δεδομένων και της ιδιωτικής ζωής. Αντ' αυτού, οι ΗΠΑ βασίζονται στην ευρεία εξουσία της Ομοσπονδιακής Επιτροπής Εμπορίου (FTC) και των πολιτειακών αρχών που είναι επιφορτισμένες με την αρμοδιότητα επιβολής των πολιτειακών νόμων για την προστασία των δεδομένων (Calia, 2022).

3.1.2 Η νομοθεσία σε ομοσπονδιακό επίπεδο

Στις Ηνωμένες Πολιτείες Αμερικής, η προστασία των προσωπικών δεδομένων διασφαλίζεται μέσω διαφορετικών ομοσπονδιακών νόμων για κάθε τομέα. Ο εκάστοτε νόμος προβλέπει διαφορετικούς ορισμούς και ρυθμίσεις για τη σύννομη επεξεργασία των προσωπικών δεδομένων.

Αναφορικά με την προστασία των προσωπικών δεδομένων των πολιτών από την επεξεργασία προσωπικών δεδομένων από τις ομοσπονδιακές υπηρεσίες εφαρμόζεται ο Privacy Act, που ψηφίστηκε το 1974 ως απάντηση στις αυξανόμενες ανησυχίες για την κυβερνητική παρακολούθηση (Calia, 2022). Ο νόμος αυτός αποτελεί ορόσημο της νομοθεσίας στις Ηνωμένες Πολιτείες, για την προστασία των δικαιωμάτων ιδιωτικής ζωής των ατόμων μέσω της ρύθμισης της συλλογής, της χρήσης και της αποκάλυψης προσωπικών πληροφοριών από ομοσπονδιακές υπηρεσίες.

Ο Privacy Act ισχύει για τις ομοσπονδιακές υπηρεσίες και διέπει τη συλλογή, τη διατήρηση, τη χρήση και τη διάδοση προσωπικών πληροφοριών που διατηρούνται σε συστήματα αρχείων από τις ομοσπονδιακές υπηρεσίες. Οι ομοσπονδιακές υπηρεσίες υποχρεούνται να προσδιορίζουν τους σκοπούς για τους οποίους συλλέγονται οι προσωπικές πληροφορίες και να περιορίζουν τη χρήση τους στους συγκεκριμένους σκοπούς. Οι αρχές δεν μπορούν να κοινοποιήσουν προσωπικές πληροφορίες χωρίς τη συγκατάθεση του ατόμου, εκτός εάν επιτρέπεται από το νόμο ή για συγκεκριμένους σκοπούς. Τα άτομα έχουν το δικαίωμα πρόσβασης και τροποποίησης των πληροφοριών που τηρούνται από ομοσπονδιακές υπηρεσίες, διασφαλίζοντας την ακρίβεια και την πληρότητα των προσωπικών τους πληροφοριών. Τέλος, οι ομοσπονδιακές υπηρεσίες πρέπει να θεσπίζουν κατάλληλες διοικητικές και τεχνικές εγγυήσεις για την προστασία της ασφάλειας και της εμπιστευτικότητας των προσωπικών πληροφοριών που έχουν στην κατοχή τους (Hoang, 2012).

Στον τομέα της υγείας, εφαρμόζεται ο Health Insurance Portability and Accountability Act (HIPAA), που υιοθετήθηκε το 1996 και θεσπίζει εθνικά πρότυπα για την προστασία των ιατρικών αρχείων και άλλων προσωπικών πληροφοριών υγείας που κατέχονται από παρόχους υγείας. Σκοπός του HIPPA είναι η διασφάλιση ότι τα ευαίσθητα δεδομένα υγείας των ατόμων παραμένουν ασφαλή, απαιτώντας τη συγκατάθεση και τη γνώση του ατόμου πριν από οποιαδήποτε αποκάλυψη. Επιπροσθέτως, ο HIPAA θεσπίζει πρότυπα για την ασφάλεια των ηλεκτρονικών προστατευμένων πληροφοριών υγείας, απαιτώντας από τους καλυμμένους φορείς να εφαρμόσουν διοικητικά, φυσικά και τεχνικά μέτρα προστασίας από την μη εξουσιοδοτημένη πρόσβαση, χρήση ή αποκάλυψη των ηλεκτρονικών προστατευμένων πληροφοριών υγείας (Moore & Frye, 2019).

Ταυτόχρονα, διαφυλάσσεται η συνεχής διάδοση ακριβών πληροφοριών για την υγεία, προκειμένου να παρέχονται και να υποστηρίζονται εξαιρετικές υπηρεσίες υγειονομικής περίθαλψης, διασφαλίζοντας παράλληλα την υγεία και την ευημερία των ατόμων. Το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών των Ηνωμένων Πολιτειών (United States Department of Health and Human Services - HHS) εξέδωσε κανονισμούς (Κανόνας Ασφαλείας - Κανόνας Προστασίας Προσωπικών Δεδομένων), με τους οποίους παρέχονται οδηγίες για την ορθή εφαρμογή του HIPAA. Η μη συμμόρφωση με τον HIPAA επισύρει πρόστιμα και άλλες νομικές συνέπειες. Τέλος, ο HIPAA απαιτεί από τους παρόχους υγείας να ειδοποιούν

τα ενδιαφερόμενα άτομα, το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών των Ηνωμένων Πολιτειών (United States Department of Health and Human Services - HHS) και, σε ορισμένες περιπτώσεις, τα μέσα ενημέρωσης, σε περίπτωση παραβίασης των ηλεκτρονικών προστατευμένων πληροφοριών υγείας (Moore & Frye, 2019).

Οι αρχές ιδιωτικότητας και ασφάλειας που κατοχυρώνονται στον HIPAA ευθυγραμμίζονται με τα διεθνή πλαίσια προστασίας δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της ΕΕ, υποδεικνύοντας μία σύγχρονη παγκόσμια τάση για τη ρύθμιση της προστασίας των προσωπικών δεδομένων, ιδίως σε ευαίσθητους τομείς όπως η υγεία. Παρόλο που θεσπίστηκε δύο δεκαετίες πριν από τον GDPR στην Ευρώπη, αυτός ο νόμος έχει πολλές ομοιότητες με τον Κανονισμό και θεωρείται ευρέως ως ο αμερικανικός ομοσπονδιακός νόμος που αντανακλά τις αρχές του (Tovino, 2017).

Παρά τα πολλά κοινά χαρακτηριστικά μεταξύ του GDPR και του HIPAA, η κύρια διαφοροποίηση έγκειται στο γεγονός ότι ο GDPR στοχεύει πρωτίστως στη διαφύλαξη των προσωπικών δεδομένων ατόμων από την Ευρωπαϊκή Ένωση, πράγμα που σημαίνει ότι κάθε οργανισμός που ασχολείται με τις πληροφορίες ενός ασθενούς εντός της ΕΕ πρέπει να συμμορφώνεται με τους κανονισμούς GDPR. Από την άλλη πλευρά, ο HIPAA εστιάζει στις οντότητες και οργανισμούς στις ΗΠΑ που χειρίζονται πληροφορίες υγείας. Συνεπώς, ο GDPR έχει μεγαλύτερο εύρος κάλυψης σε σύγκριση με το HIPAA. Επιπλέον, ενώ ο HIPAA επιτρέπει ορισμένες αποκαλύψεις προσωπικών στοιχείων των ασθενών χωρίς τη συγκατάθεσή τους, ο GDPR απαιτεί ρητή συναίνεση για τέτοιες ενέργειες (Tovino, 2017).

Στον τομέα τηλεπικοινωνιών, θεσπίστηκε το 1991 ο Federal Telephone Consumer Protection Act (TCPA), ένας ομοσπονδιακός Νόμος, που διέπει τη χρήση συστημάτων τηλεφωνικών κλήσεων και τεχνητών ή προηχογραφημένων φωνών στις τηλεπικοινωνίες. Πρωταρχικός στόχος του TCPA είναι να περιορίσει τη χρήση αυτοματοποιημένων ή προηχογραφημένων κλήσεων, τόσο σε σταθερά όσο και σε κινητά τηλέφωνα, εκτός εάν ο παραλήπτης έχει δώσει τη ρητή συγκατάθεσή του ή εάν η κλήση γίνεται για λόγους έκτακτης ανάγκης. Αξιοσημείωτο είναι ότι τα δικαιώματα που παρέχει ο νόμος εκτείνονται όχι μόνο σε μεμονωμένους καταναλωτές αλλά και σε νομικές οντότητες (Cain, 1993).

Επιπροσθέτως, ο TCPA απαγορεύει σε διάφορες οντότητες, συμπεριλαμβανομένων των τηλεπωλητών, χρηματοπιστωτικών ιδρυμάτων, εισπρακτικών εταιρειών και άλλων επιχειρήσεων να χρησιμοποιούν Συστήματα Αυτόματης Τηλεφωνικής Κλήσης (ATDS), να επικοινωνούν με καταναλωτές στα κινητά τους τηλέφωνα χωρίς να έχουν παράσχει τη συγκατάθεσή τους. Το ATDS αναφέρεται σε εξοπλισμό που διαθέτει τη δυνατότητα αποθήκευσης ή δημιουργίας τηλεφωνικών αριθμών με δυνατότητα κλήσης, χρησιμοποιώντας είτε μια γεννήτρια τυχαίων είτε διαδοχικών αριθμών και στη συνέχεια να καλεί αυτούς τους αριθμούς. Κατά την αξιολόγηση του κατά πόσον ένα σύστημα πληροί τις προϋποθέσεις ως ATDS, τόσο η FTC όσο και τα δικαστήρια εξετάζουν συχνά την ικανότητά του να πραγματοποιεί κλήσεις χωρίς ανθρώπινη συμμετοχή ως βασικό παράγοντα εξέτασης (Cain, 1993).

Στον τομέα των χρηματοοικονομικών, ο πρώτος νόμος ήταν ο Fair Credit Reporting Act (FCRA), που θεσπίστηκε το 1970 και αργότερα τροποποιήθηκε από τον Fair and Accurate Credit Transactions Act (FACTA). Ο FCRA είναι ιδιαίτερα σημαντικός για το αμερικανικό

σύστημα προστασίας των δεδομένων, καθώς αποτέλεσε τη βάση για τη σύγχρονη νομοθεσία για την προστασία της ιδιωτικής ζωής της «ειδοποίησης και συναίνεσης» και της «πρόσβασης στις πληροφορίες» (Hoang, 2012). Πιο συγκεκριμένα, ο FCRA επιτρέπει σε ένα πιστωτικό οργανισμό να διαβιβάζει μία πιστωτική έκθεση που περιέχει προσωπικές πληροφορίες προκειμένου να προσδιοριστεί η επιλεξιμότητα του ατόμου για πίστωση, ασφάλιση ή απασχόληση, ωστόσο, ο νόμος απαιτεί από τον πιστωτικό οργανισμό να λαμβάνει εύλογα μέτρα για να διασφαλίσει την ακρίβεια, τη συνάφεια και την ορθή χρήση των πληροφοριών. Ο FCRA ρυθμίζει τις παραδοσιακές καθώς και τις επιγραμμικές δραστηριότητες αναφοράς πιστώσεων. Ορισμένοι θεωρητικοί έχουν υποστηρίξει ότι ο FCRA προσεγγίζει το απόρρητο των δεδομένων χρησιμοποιώντας μια «ψευδο-συμβατική» προσέγγιση στην προστασία των δεδομένων, επιτρέποντας στους πελάτες να αλλάξουν το πεδίο εφαρμογής της σχέσης τους με τους οργανισμούς αναφοράς πιστοληπτικής ικανότητας (Hoang, 2012 & Sobel 2008).

Ο Gramm-Leach Bliley (GLBA), επίσης γνωστός ως Financial Modernization Act of 1999, αποτελεί μια σημαντική νομοθετική πρωτοβουλία στις Ηνωμένες Πολιτείες με στόχο τον κανονισμό του χρηματοπιστωτικού τομέα και την ενίσχυση της προστασίας της ιδιωτικότητας των καταναλωτών. Ο GLBA αποτελείται από βασικές διατάξεις που στοχεύουν στην προστασία των χρηματοπιστωτικών πληροφοριών. Στο νόμο αυτό, οι προσωπικές πληροφορίες που προστατεύονται αφορούν τις προσωπικά αναγνωρίσιμες οικονομικές πληροφορίες, που παρέχονται από τον καταναλωτή σε χρηματοπιστωτικό ίδρυμα και που προκύπτουν από συναλλαγή με τον καταναλωτή (Boyne. 2018).

Ο GLBA υποχρεώνει τα χρηματοπιστωτικά ιδρύματα να ενημερώνουν τους πελάτες τους σχετικά με τις πρακτικές κοινοποίησης πληροφοριών και να παρέχουν μηχανισμούς επιλογής για την κοινοποίηση ιδιωτικών προσωπικών πληροφοριών με τρίτους. Υπό το καθεστώς του GLBA, τα χρηματοπιστωτικά ιδρύματα υποχρεούνται να αναπτύξουν και να εφαρμόσουν πλήρη προγράμματα ασφαλείας για την προστασία των ευαίσθητων πληροφοριών των πελατών από μη εξουσιοδοτημένη πρόσβαση, χρήση ή κοινοποίηση. Τα χρηματοπιστωτικά ιδρύματα μπορούν να διαβιβάσουν προσωπικές πληροφορίες σε τρίτες εταιρείες μόνο εφόσον είναι αναγκαίο για τις παρεχόμενες οικονομικές υπηρεσίες (Boyne, 2018).

Η έμφαση του GLBA στη διαφάνεια, τη συγκατάθεση του καταναλωτή και την ασφάλεια δεδομένων συμβαδίζει με ευρύτερα διεθνή πλαίσια προστασίας δεδομένων, προάγοντας μια σύγχρονη σύγκλιση παγκόσμιων κανονισμών όσον αφορά την προστασία των προσωπικών δεδομένων. Ο GLBA έχει έναν βαθύ αντίκτυπο στον χρηματοπιστωτικό τομέα στις Ηνωμένες Πολιτείες, προάγοντας μεγαλύτερη διαφάνεια, ευθύνη και εμπιστοσύνη στη χειριστή των χρηματοπιστωτικών ιδρυμάτων σχετικά με τις προσωπικές πληροφορίες των καταναλωτών. Μέσω της απαίτησης ισχυρών προτύπων ιδιωτικότητας και ασφάλειας, ο GLBA έχει συμβάλει στην ανάπτυξη βέλτιστων πρακτικών για την προστασία δεδομένων και την κυβερνοασφάλεια στον χρηματοπιστωτικό τομέα, παρόλο που από ορισμένους θεωρητικούς έχει χαρακτηριστεί ένας προβληματικός νόμος, που δεν παρέχει επαρκή προστασία για τα προσωπικά δεδομένα (Janger & Schwartz, 2002).

Αναφορικά με την προστασία των δεδομένων των παιδιών στο διαδίκτυο, έχει υιοθετηθεί ο Children's Online Privacy Protection Act (COPPA) του 1998, ως απάντηση στην

εκθετική επέκταση των στρατηγικών ψηφιακού μάρκετινγκ που απευθύνονται σε παιδιά κατά τα τέλη της δεκαετίας του 1990. Κατά τη διάρκεια αυτής της περιόδου, οι ιστότοποι συγκέντρωναν πληροφορίες από ανήλικα άτομα χωρίς να λάβουν την απαραίτητη συγκατάθεση από τους γονείς τους (Topelson, Bavitz, Cupta & Oberman, 2013). Ο COPPA εφαρμόζεται αποκλειστικά στα δεδομένα παιδιών κάτω των δεκατριών ετών, που συλλέγονται και τυγχάνουν επεξεργασίας μέσω του Διαδικτύου. Ο Νόμος περιέχει έναν αξιοσημείωτο περιορισμό σχετικά με το τι θεωρούνται προσωπικές πληροφορίες. Συγκεκριμένα, ως προσωπική πληροφορία προσδιορίζεται το όνομα και το επώνυμο του ανηλίκου τέκνου, ο τόπος διαμονής του, η διεύθυνση ηλεκτρονικού ταχυδρομείου, ο αριθμός τηλεφώνου, ο αριθμός κοινωνικής ασφάλισης ή οποιεσδήποτε λεπτομέρειες σχετικά με το παιδί ή τους γονείς του. Στο πλαίσιο του COPPA, χρησιμοποιείται ο όρος «operator», που περιλαμβάνει τόσο τον υπεύθυνο επεξεργασίας όσο και τον εκτελών την επεξεργασία που υπάρχουν στον GDPR. Ως «operator» αναφέρεται κάθε φυσικό ή νομικό πρόσωπο, που διαχειρίζεται έναν ιστότοπο ή μια διαδικτυακή υπηρεσία που βρίσκεται στο Διαδίκτυο και προβαίνει συλλογή ή τη διατήρηση προσωπικών πληροφοριών από χρήστες ή για λογαριασμό των χρηστών, κατά την προσφορά προϊόντων ή υπηρεσιών (Topelson, Bavitz, Cupta & Oberman, 2013).

Οι ρυθμίσεις που περιγράφονται στο COPPA παρέχουν σαφείς οδηγίες για τους χειριστές ιστότοπων, τους εμπόρους και άλλους παρόχους ηλεκτρονικών υπηρεσιών για τη διασφάλιση της ασφάλειας των προσωπικών πληροφοριών. Μία από τις κεντρικές απαιτήσεις του COPPA είναι η υποχρέωση των εκδοτών ιστοσελίδων και των παρόχων διαδικτυακών υπηρεσιών να λαμβάνουν συγκατάθεση των γονέων πριν από τη συλλογή, τη χρήση ή τη διάθεση προσωπικών πληροφοριών από παιδιά κάτω των 13 ετών. Ο COPPA απαιτεί από τους παρόχους να διατηρούν σαφείς και συνεκτικές πολιτικές απορρήτου που περιγράφουν τις πρακτικές συλλογής δεδομένων τους, συμπεριλαμβανομένων των τύπων πληροφοριών που συλλέγονται, του τρόπου χρήσης τους και των ατόμων με τα οποία μοιράζονται. Ο COPPA επιβάλλει την εφαρμογή λογικών μέτρων ασφαλείας για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των προσωπικών πληροφοριών των παιδιών που συλλέγονται στο διαδίκτυο (Topelson, Bavitz, Cupta & Oberman, 2013).

Αναφορικά με τη μη ζητηθείσα ηλεκτρονική επικοινωνία εφαρμόζεται ο Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003, που αφορά τα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου. Ως εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου ορίζονται κάθε μήνυμα ηλεκτρονικού ταχυδρομείου, του οποίου πρωταρχικός σκοπός είναι η εμπορική διαφήμιση ή προώθηση ενός εμπορικού προϊόντος (Boyne, 2018).

Σύμφωνα με τον CAN-SPAM Act, όλοι οι οργανισμοί, απαγορεύεται να αποστέλλουν μηνύματα ηλεκτρονικού ταχυδρομείου με ουσιωδώς ψευδείς, παραπλανητικές ή παραπλανητικές πληροφορίες. Σε περίπτωση που ένα μήνυμα ηλεκτρονικού ταχυδρομείου αποτελεί διαφήμιση ή πρόσκληση, πρέπει να προσδιορίζεται σαφώς. Επιπλέον, το email θα πρέπει να περιέχει σαφή και κατανοητή επισήμανση αναφορικά με τη δυνατότητα εναντίωσης στη λήψη μελλοντικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από τον αποστολέα, και πρέπει να περιλαμβάνει κάποια διεύθυνση ηλεκτρονικού ταχυδρομείου ή άλλο μηχανισμό με τον οποίο ο παραλήπτης μπορεί να είναι σε θέση να εξαιρεθεί (Boyne,

2018). Ο CAN-SPAM Act επιβάλλεται από την Ομοσπονδιακή Επιτροπή Εμπορίου, βάσει της αρμοδιότητάς της να αποτρέπει αθέμιτες και παραπλανητικές εμπορικές πρακτικών σύμφωνα με τον Fair Trade Commission Act (Boyne, 2018).

Για την εφαρμογή των προαναφερθέντων νόμων, σημαντικό ρόλο διαδραματίζουν οι εκάστοτε φορείς επιβολής των ομοσπονδιακών νόμων. Η Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission) είναι ο κύριος φορέας επιβολής των ομοσπονδιακών νόμων για την προστασία της ιδιωτικής ζωής. Ο νόμος της Ομοσπονδιακής Επιτροπής Εμπορίου, Fair Trade Commission Act απαγορεύει τις αθέμιτες ή παραπλανητικές πρακτικές και έχει εφαρμοστεί και στην ιδιωτικότητα και την ασφάλεια των δεδομένων στο διαδίκτυο και εκτός διαδικτύου. Το Γραφείο Πολιτικών Δικαιωμάτων (Office of Civil Rights -OCR) του Υπουργείου Υγείας και Ανθρωπίνων Υπηρεσιών είναι υπεύθυνο για την επιβολή του Health Insurance Portability and Accountability Act (HIPAA). Αρμοδιότητα εφαρμογής και θέσπισης κανόνων για τον νόμο Gramm-Leach-Bliley Act (GLBA) για τις διατάξεις περί προστασίας της ιδιωτικής ζωής μοιράζονταν προηγουμένως οκτώ ομοσπονδιακοί φορείς. Ωστόσο, επί του παρόντος, η επιβολή έχει ανατεθεί στην Αρχή Οικονομικής Προστασίας Καταναλωτών (Consumer Financial Protection Agency - CFPB), (Rustad, 2019).

3.1.3 Η νομοθεσία σε επίπεδο πολιτειών

Παρά το γεγονός ότι όπως αναφέρθηκε ανωτέρω δεν υπάρχει ομοιόμορφο και ικανοποιητικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων στις ΗΠΑ, κάποιες πολιτείες των ΗΠΑ έχουν ακολουθήσει το πρότυπο της ΕΕ και έχουν υιοθετήσει αντίστοιχους κανόνες στον τομέα των προσωπικών δεδομένων. Συνολικά 15 μόνο Πολιτείες, έχουν υιοθετήσει ολοκληρωμένο και σαφές νομικό πλαίσιο, ενώ οι υπόλοιπες είτε έχουν σχετική νομοθεσία με στενότερο προστατευτικό πλαίσιο, είτε έχουν κατατεθεί νομοσχέδια, χωρίς ακόμη να έχουν ψηφιστεί[22].

Η Καλιφόρνια ήταν η πρώτη Πολιτεία που θέσπισε ολοκληρωμένη νομοθεσία περί απορρήτου δεδομένων μέσω του California Consumer Privacy Act (CCPA) και του California Privacy Rights Act (CPRA) και διαθέτει ένα από τα πλέον πλήρη νομικά πλαίσια για την προστασία των δεδομένων στις Ηνωμένες Πολιτείες, θέτοντας υψηλά πρότυπα για τη διαφύλαξη των προσωπικών πληροφοριών των ατόμων. Ο CCPA, που υπεγράφη στις 8 Ιουνίου 2018 και τέθηκε σε ισχύ την 1η Ιανουαρίου 2020, θεσπίζει δικαιώματα απορρήτου και απαιτήσεις για τη συλλογή και την πώληση προσωπικών πληροφοριών των πολιτών της Καλιφόρνια. Στις 3 Νοεμβρίου 2020, οι ψηφοφόροι της Καλιφόρνια ενέκριναν τον CPRA, ο οποίος τροποποίησε και επέκτεινε το CCPA. Ο CPRA τέθηκε σε ισχύ στις 16 Δεκεμβρίου 2020 – αν και οι περισσότερες από τις αναθεωρήσεις του CCPA τέθηκαν σε ισχύ την 1η Ιανουαρίου 2023 (Pardau, 2018).

Το νομικό αυτό πλαίσιο, ακολουθεί σε μεγάλο βαθμό το πρότυπο του GDPR με διάφορους τρόπους, καθιστώντας την πιο αξιοσημείωτη πολιτειακή νομοθεσία για την προστασία της ιδιωτικής ζωής των δεδομένων στις ΗΠΑ (Field E., 2020). Σε αντίθεση με τους περισσότερους ομοσπονδιακούς και πολιτειακούς νόμους του είδους της, η συγκεκριμένη νομοθεσία προστατεύει όχι μόνο τον καταναλωτή, αλλά και το άτομο σε όλες τις εγγενείς

[22] US Privacy Laws. https://www.dataguidance.com/comparisons/usa-privacy-laws (Τελευταία προσπέλαση: 21 Μαρτίου 2024)

ιδιότητές τους, με μόνη μερική εξαίρεση τους «ασθενείς» που προστατεύονται από την HIPAA (Pardau, 2018).

Τόσο ο CCPA όσο και ο CPRA χορηγούν στους καταναλωτές εκτεταμένα δικαιώματα σχετικά με τα προσωπικά τους δεδομένα, συμπεριλαμβανομένου του δικαιώματος να μάθουν ποιες πληροφορίες συλλέγονται, πωλούνται ή αποκαλύπτονται για αυτούς, το δικαίωμα πρόσβασης στα δεδομένα τους και το δικαίωμα να ζητήσουν τη διαγραφή των δεδομένων του. Απαιτούν από τις επιχειρήσεις να παρέχουν διαφανείς αποκαλύψεις σχετικά με τις πρακτικές συλλογής δεδομένων και να λαμβάνουν σαφή συγκατάθεση για τη συλλογή και επεξεργασία ευαίσθητων πληροφοριών. Ο CCPA και ο CPRA επιβάλλουν στις επιχειρήσεις την υλοποίηση κατάλληλων μέτρων ασφαλείας για την προστασία των προσωπικών δεδομένων των καταναλωτών από μη εξουσιοδοτημένη πρόσβαση ή την καταστροφή. Και οι δύο νόμοι εισάγουν μηχανισμούς με τους οποίους μπορούν οι καταναλωτές να στραφούν εναντίον των επιχειρήσεων για παραβιάσεις των δικαιωμάτων τους στην ιδιωτικότητα. Επιπλέον, ιδρύουν οργανισμούς ελέγχου, όπως το Γραφείο του Γενικού Εισαγγελέα της Καλιφόρνια (California Office of the Attorney General), που είναι υπεύθυνο για την επίβλεψη της συμμόρφωσης των επιχειρήσεων με τους CCPA και CPRA και την επιβολή κυρώσεων (Pardau, 2018).

Λίγο μετά την ψήφιση της CCPA από την Καλιφόρνια, η Νέα Υόρκη θέσπισε επίσης έναν ολοκληρωμένο νόμο για την προστασία της ιδιωτικής ζωής των δεδομένων, το Stop Hacks and Electronic Data Security Act («SHIELD Act»), ακολουθώντας τον GDPR. Ο νόμος SHIELD Act αντιμετωπίζει θέματα προστασίας της ιδιωτικής ζωής των δεδομένων που τονίζονται στον GDPR, αλλά διαφέρει ως προς την προσέγγισή του για τα χρηματοπιστωτικά ιδρύματα.

Μία ακόμη Πολιτεία που έχει υιοθετήσει ένα ολοκληρωμένο νομοθέτημα για την προστασία των δεδομένων στις ΗΠΑ είναι το Κολοράντο που θέσπισε τον Colorado Privacy Act (CPA) τον Ιούλιο του 2021. Ο CPA χορηγεί στους καταναλωτές διάφορα δικαιώματα σχετικά με τα προσωπικά τους δεδομένα, συμπεριλαμβανομένου του δικαιώματος να αποκλείσουν την επεξεργασία των δεδομένων τους, να έχουν πρόσβαση και να διορθώσουν τα δεδομένα τους και να ζητήσουν τη διαγραφή των δεδομένων τους (Gerke & Rezaeikhonakdar, 2022).

Ο CPA επιβάλλει περιορισμούς στη συλλογή, τη χρήση και την κοινοποίηση των προσωπικών δεδομένων από τις επιχειρήσεις. Απαιτεί από τις επιχειρήσεις να παρέχουν σαφείς και διαφανείς ανακοινώσεις σχετικά με τις πρακτικές τους για τα δεδομένα και να λάβουν ρητή συγκατάθεση για την επεξεργασία ευαίσθητων δεδομένων. Επιβάλλει στις επιχειρήσεις να υλοποιήσουν λογικά μέτρα ασφαλείας και διαδικασίες για την προστασία των προσωπικών δεδομένων των καταναλωτών από μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, αλλοίωση ή καταστροφή. Επιπροσθέτως, ο CPA αυτός θεσπίζει το Γραφείο του Γενικού Εισαγγελέα του Κολοράντο (Colorado Office of the Attorney General), ως την κύρια αρχή επιβολής, υπεύθυνη για την επίβλεψη της συμμόρφωσης των επιχειρήσεων με τον νόμο. Τέλος, παρέχει μέσα για τους καταναλωτές να υποβάλουν παράπονα σχετικά με παραβιάσεις των δικαιωμάτων τους στην ιδιωτικότητα και επιτρέπει στον Γενικό Εισαγγελέα να διερευνήσει και να επιβάλλει κυρώσεις εναντίον των μη συμμορφούμενων επιχειρήσεων (Gerke & Rezaeikhonakdar, 2022).

3.2 Η σύγκριση του Νόμου της Καλιφόρνια περί Προστασίας των Καταναλωτών (CCPA) και του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR)

3.2.1 Εδαφικό πεδίο εφαρμογής και βασικοί ορισμοί

Όπως αναφέρθηκε ανωτέρω, η προστασία των προσωπικών δεδομένων στις ΗΠΑ, διαφέρει αρκετά σε σχέση με το νομικό πλαίσιο της ΕΕ, καθώς αυτή διασφαλίζεται μέσω διαφορετικών νόμων σε ομοσπονδιακό και πολιτειακό επίπεδο. Ωστόσο, ο πιο ολοκληρωμένος και σαφής νόμος θεωρείται California Consumer Privacy Act (CCPA). Ως εκ τούτου, στη συνέχεια θα επιχειρηθεί μία σύγκριση του νόμου αυτού με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).

Αναφορικά με την εδαφική εμβέλεια του GDPR, το εδαφικό πεδίο εφαρμογής εκτείνεται πέραν των φυσικών συνόρων των κρατών μελών της ΕΕ. Σύμφωνα με τον GDPR, κατ' αρχήν οι εταιρείες ή οποιεσδήποτε άλλες οντότητες που εδρεύουν στην επικράτεια της ΕΕ υπόκεινται στον κανονισμό για δραστηριότητες επεξεργασίας δεδομένων[23]. Ωστόσο, ορίζεται επίσης ότι ανεξάρτητα από την εγκατάσταση της εταιρείας, εάν η αυτή προσφέρει αγαθά και υπηρεσίες ή παρακολουθεί τη συμπεριφορά των ατόμων εντός της ΕΕ, θα υπόκειται στον GDPR για την επεξεργασία των δεδομένων των πολιτών της ΕΕ[24].

Ομοίως, σύμφωνα με τον CCPA, οι οντότητες που ασκούν επιχειρηματική δραστηριότητα στην Πολιτεία της Καλιφόρνια υπόκεινται στη νομοθεσία, ανεξάρτητα από την εγκατάστασή τους, όταν επεξεργάζονται τα δεδομένα των πολιτών των κατοίκων της Καλιφόρνιας[25]. Η διάταξη αυτή βρίσκεται σε συνάρτηση με εκείνη του GDPR, ωστόσο ο CCPA δεν εφαρμόζεται σε οντότητες που δεν ασκούν επιχειρηματική δραστηριότητα στην Καλιφόρνια, ακόμη και αν αυτές παρακολουθούν τους κατοίκους της Καλιφόρνια (Lydia de la Torre, 2018).

Σε γενικές γραμμές, παρόλο που το πεδίο εφαρμογής της CCPA φαίνεται να είναι σχετικά στενότερο σε σύγκριση με τον GDPR, οι δύο νομοθεσίες παρουσιάζουν συνολικά παρόμοια αντιμετώπιση όσον αφορά την (εσωτερική και εξωτερική) εδαφικότητα (Calzada, 2022).

Εν συνεχεία, διαφορές παρουσιάζονται αναφορικά με τους βασικούς ορισμούς των δύο νομοθετημάτων. Αρχικά, σύμφωνα με τον GDPR, ο όρος δεδομένα προσωπικού χαρακτήρα ορίζεται ως «κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)[26]». Ενώ, ο όρος επεξεργασία ορίζεται ως: «Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη

[23] GDPR, άρθρο 3 παρ. 1
[24] GDPR, άρθρο 3 παρ. 2
[25] Cal. Civ. Code, §1798.140 (c)(1))
[26] GDPR, άρθρο 4 αρ. 1

μορφή διάθεσης, η συσχέτιση, ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή[27]».

Στο νόμο CCPA, τα δεδομένα προσωπικού χαρακτήρα χαρακτηρίζονται ως «προσωπικές πληροφορίες» και ορίζονται ως «πληροφορίες που ταυτοποιούν, συσχετίζουν, περιγράφουν, είναι ευλόγως ικανές να αποτελέσουν να συσχετιστούν ή θα μπορούσαν εύλογα να συνδεθούν, άμεσα ή έμμεσα, με ένα συγκεκριμένο καταναλωτή ή νοικοκυριό[28]». Παρόλο που ο ορισμός των προσωπικών δεδομένων/πληροφοριών του GDPR και του CCPA είναι παρόμοιοι, διαφέρουν κυρίως ως προς ότι ο ορισμός του CCPA, περιλαμβάνει έξω-προσωπικά δεδομένα, δηλαδή όχι μόνο δεδομένα που αφορούν συγκεκριμένα άτομα αλλά και νοικοκυριά (Jehl & Friel, 2018).

Εξάλλου, αντιστοίχως με τον GDPR, ο CCPA ορίζει την επεξεργασία ως «κάθε πράξη ή σύνολο πράξεων που εκτελούνται σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, με ή χωρίς αυτοματοποιημένα μέσα»[29]. Ωστόσο, απουσιάζουν οι ειδικότερες κατηγορίες, που αναφέρονται στο πλαίσιο του GDPR, οι οποίες αποτελούν παραδείγματα μιας τέτοιας ενέργειας.

Συνολικά, ο CCPA ορίζει τα προσωπικά δεδομένα ελαφρώς διαφορετικά, καθώς περιλαμβάνει και εξω--προσωπικά δεδομένα, ενώ έχει στενότερη κατηγοριοποίηση της επεξεργασίας σε σύγκριση με τον GDPR. Παρά τις διαφορές αυτές, μπορεί να υποστηριχθεί ότι οι ορισμοί τόσο των δεδομένων προσωπικού χαρακτήρα όσο και της επεξεργασίας είναι ουσιαστικά τους παρόμοιοι στις δύο νομοθεσίες (Amdahl, 2023).

3.2.2 Η συγκατάθεση

Αναφορικά με τη συγκατάθεση, υφίστανται δύο καθεστώτα, η συγκατάθεση opt-in και η συγκατάθεση opt-out. Ειδικότερα, υπό το καθεστώς opt-in, απαιτείται από τους διαδικτυακούς εμπορικούς οργανισμούς να λαμβάνουν τη ρητή, θετική και κατόπιν ενημέρωσής του, συγκατάθεση του ατόμου προτού προβούν σε επεξεργασία δεδομένων. Αντιθέτως, υπό το καθεστώς συγκατάθεσης opt-out, δεν απαιτείται να λαμβάνεται ρητή και συγκεκριμένη συγκατάθεση πριν την επεξεργασία, αλλά υφίσταται η δυνατότητα του υποκειμένου να ζητήσει να εξαιρεθεί από την επεξεργασία δεδομένων του (Park, 2020).

Παρόλο που ο GDPR δεν χρησιμοποιεί ρητά τον όρο «opt-in», ο ορισμός που δίδεται για τη συγκατάθεση σε συνδυασμό με τις προϋποθέσεις που απαιτούνται για έγκυρη συγκατάθεση, προσιδιάζουν ουσιαστικά στη συγκατάθεση opt-in πριν από την επεξεργασία δεδομένων. Ειδικότερα, ο GDPR ορίζει τη συγκατάθεση ως «κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη 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[30]»

Αντιθέτως, ο CCPA δεν υιοθετεί το καθεστώς opt-in του GDPR, αλλά προβλέπει ένα καθεστώς εξαίρεσης. Ο CCPA παρέχει στους καταναλωτές το δικαίωμα να «εξαιρεθούν»

[27] GDPR, άρθρο 4 αρ. 2
[28] Cal. Civ. Code §1798.140 (o)(1))
[29] Cal. Civ. Code §1798.140 (o)(2))
[30] GDPR, άρθρο 4 παρ. 11

από μια επιχείρηση που πωλεί τις προσωπικές τους πληροφορίες σε τρίτους[31]. Ειδικότερα, οι επιχειρήσεις πρέπει να παρέχουν ειδοποίηση ότι οι πληροφορίες που συλλέγονται μπορούν να πωληθούν και ότι οι καταναλωτές έχουν το δικαίωμα να αρνηθούν την πώληση των προσωπικών τους πληροφοριών. Κατά την εξέταση των κειμένων του CCPA και του GDPR, γίνεται εύκολα αντιληπτό ότι η διάταξη περί opt-out στον CCPA δεν προστατεύει τους καταναλωτές ισοδύναμα με τη συγκατάθεση opt-in στον GDPR και η διαφορά αυτή είναι η πιο σημαντική διαφοροποίηση μεταξύ των δύο νόμων (Park, 2020).

3.2.3 Εφαρμογή της νομοθεσίας και επιβολή κυρώσεων

Τέλος, διαφορετική προσέγγιση στους δύο δικαιοδοσίας υπάρχει και αναφορικά με τον τρόπο με τον οποίο κάθε δικαιοδοσία επιβάλλει τη νομοθεσία της σε οντότητες που δε συμμορφώνονται με τις υποχρεώσεις τους ως διαχειριστές δεδομένων.

Κατ' αρχήν, ο GDPR ενισχύει την εποπτική ανεξαρτησία μέσω των Αρχών Προστασίας Δεδομένων (ΑΠΔ). Οι ΑΠΔ εποπτεύουν, μέσω ερευνητικών και διορθωτικών εξουσιών, την εφαρμογή της νομοθεσίας για την προστασία των δεδομένων και, για το λόγο αυτό, υπάρχει μία σε κάθε κράτος μέλος της ΕΕ. Κάθε φορά που οι ΑΠΔ διαπιστώσουν παραβιάσεις του GDPR, εκτός από τις διορθωτικές εξουσίες τους, μπορούν επίσης να επιβάλλουν διοικητικά πρόστιμα. Τα διοικητικά πρόστιμα επιβάλλονται σε δύο επίπεδα με βάση τη σοβαρότητα της παράβασης. Οι λιγότερο σοβαρές παραβιάσεις υπόκεινται σε διοικητικά πρόστιμα ύψους έως δέκα εκατομμυρίων ευρώ ή έως 2% του συνολικού παγκόσμιου ετήσιου (καθαρού) κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο από τα δύο είναι υψηλότερο[32]. Ωστόσο, οι πιο σοβαρές παραβάσεις, επισύρουν διοικητικά πρόστιμα έως 20 εκατομμύρια ευρώ, ή έως 4% του του συνολικού παγκόσμιου ετήσιου (καθαρού) κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο από τα δύο είναι υψηλότερο[33] (Ambdahl, 2023).

Ομοίως με τον GDPR, ο CCPA ορίζει έναν κυβερνητικό φορέα με αρμοδιότητα επιβολής δικαιοδοσία, το γραφείο του Γενικού Εισαγγελέα της Καλιφόρνια (Lydia de la Torre, 2018). Σε περίπτωση που η εν λόγω αρχή διαπιστώσει παραβιάσεις του CCPA, ενεργοποιούνται κυρώσεις. Παρ' όλα αυτά, σε σύγκριση με τον GDPR, τα εν λόγω πρόστιμα θεωρούνται λιγότερο αποτελεσματικά, καθώς είναι σαφώς μικρότερα τα ποσά. Τα πρόστιμα, σύμφωνα με τον CCPA, μπορούν να φτάσουν μόνο μέχρι 2.500 δολάρια ΗΠΑ για κάθε μη σκόπιμη παραβίαση και έως 7.500 δολάρια ΗΠΑ για κάθε σκόπιμη παραβίαση[34] (Amdahl, 2023).

Συνοψίζοντας, η αμερικανική προσέγγιση για την προστασία της ιδιωτικής ζωής και των δεδομένων συνίσταται σε ένα συνονθύλευμα πολιτειακών και ομοσπονδιακών νόμων, ενώ δεν υπάρχει ένα ολοκληρωμένο γενικό πλαίσιο. Ως εκ τούτου, η προστασία των υποκειμένων από την επεξεργασία των προσωπικών τους δεδομένων διαφέρει από τον ένα τομέα δραστηριότητας στον άλλον και από τη μία Πολιτεία στην άλλη Πολιτεία. Ο πιο ολοκληρωμένος και σαφής νόμος θεωρείται ο California Consumer Privacy Act (CCPA), ο

[31] Cal. Civ. Code §1798.120(α)
[32] GDPR, άρθρο 83 παρ. 4
[33] GDPR, άρθρο 83 παρ. 5
[34] Cal. Civ. Code, §1798.155 (α)

οποίος αν και παρουσιάζει αρκετές ομοιότητες με τον GDPR, αποκλίνει από αυτόν σε θεμελιώδη σημεία, όπως είναι το καθεστώς συγκατάθεσης.

4. Το «Brussels Effect» στην προστασία των προσωπικών δεδομένων

Στην προσπάθεια εξήγησης του «εξευρωπαϊσμού», δηλαδή του φαινομένου κατά το οποίο χώρες εκτός Ευρωπαϊκής Ένωσης υιοθετούν αντίστοιχα ρυθμιστικά πρότυπα με την Ευρώπη, διατυπώθηκαν πολλές θεωρίες. Η πιο σημαντική είναι η θεωρία της Bradford, που επινόησε τον όρο «το Φαινόμενο των Βρυξελλών» («Brussels Effect»). Το έργο της Bradford σχετικά με το «Brussels Effect»βασίζεται στις παραπάνω θεωρίες, αλλά επιχειρεί να παράσχει μια πιο ολοκληρωμένη και αναλυτική επεξήγηση για το πώς και γιατί συντελείται αυτός ο «εξευρωπαϊσμός» των κανόνων.

4.1 Η έννοια και οι προϋποθέσεις του «Brussels Effect»

4.1.1 Η προσπάθεια εξήγησης του «εξευρωπαϊσμού» και η έννοια του «Brussels Effect»

Η πρώιμη επιστημονική προσέγγιση για τη παγκόσμια διάδοση των προτύπων της προστασίας προσωπικών δεδομένων της Ευρωπαϊκής Ένωσης, δεν ασχολήθηκε με την εξήγηση του φαινομένου. Η πρώτη συστηματική απόπειρα διερεύνησης του ζητήματος συντελέστηκε από τον Colin Bennet, ο οποίος οδηγήθηκε στη διαπίστωση ότι ενώ υφίσταται εκτεταμένη διακρατική σύγκλιση όσον αφορά την ρύθμιση της προστασίας των δεδομένων και τις βασικές αρχές των νόμων, παράλληλα παρατηρούνται σημαντικές αποκλίσεις όσον αφορά τα καθεστώτα επιβολής του νόμου (Bennett, 1992).

Ο Bennett διατύπωσε πέντε υποθέσεις για τις συνθήκες που οδήγησαν στη σύγκλιση αυτή: πρώτον, η ταύτιση των αντιλήψεων περί τεχνολογικών απειλών, η οποία ανάγκασε τους υπεύθυνους χάραξης πολιτικής να υιοθετήσουν παρόμοιες λύσεις, δεύτερον, η βούληση των φορέων χάραξης πολιτικής να αντλήσουν διδάγματα και να μιμηθούν τις πολιτικές που υιοθετήθηκαν προγενέστερα σε άλλες χώρες, τρίτον, η σύμπνοια μέρους του διακρατικού δικτύου εμπειρογνωμόνων όσον αφορά την κατάλληλη πολιτική προστασίας δεδομένων, τέταρτον, οι προσπάθειες εναρμόνισης των διεθνών οργανισμών, ιδίως του Συμβουλίου της Ευρώπης και του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), και πέμπτον, η «διείσδυση» (μια διαδικασία κατά την οποία κάποιες χώρες αναγκάζονται να υιοθετήσουν ορισμένες πολιτικές λόγω της ενέργειες άλλων χωρών), (Bennett, 1992). Έπειτα από διεξοδική του ανάλυση, ο Bennett διαπίστωσε ότι καμία από αυτές τις υποθέσεις δεν εξηγούσε από μόνη της επαρκώς τη σύγκλιση των πολιτικών, ωστόσο, είχαν σημαντική επεξηγηματική χρησιμότητα σε συνδυασμό μεταξύ τους (Bennett, 1992).

Κάποιες δεκαετίες αργότερα, οι νομικοί θεωρητικοί, αναζητώντας μια βαθύτερη εξήγηση για την επικράτηση των ευρωπαϊκών πολιτικών προτιμήσεων στον καθορισμό των προτύπων προστασίας δεδομένων σε μη ευρωπαϊκές περιοχές, έτειναν να καταλήξουν αρχικά σε δύο κύριες αιτίες: αφενός, στο μεγάλο μέγεθος και τη διεθνή ελκυστικότητα της εσωτερικής αγοράς της ΕΕ και, αφετέρου, στην ιδιαίτερη ανησυχία της ΕΕ για τη διατήρηση υψηλών επιπέδων προστασίας των δεδομένων (Goldsmith & Wu, 2006).

Αντιθέτως, οι Newman και Bach, υποστήριξαν ότι η μεγάλη και ελκυστική κλίμακα της εσωτερικής αγοράς της ΕΕ αποτελεί αναγκαία μεν, αλλά ανεπαρκή προϋπόθεση για τη διεθνή κανονιστική ισχύ της ΕΕ, ενώ επεσήμαναν ότι εξίσου σημαντική είναι η «κανονιστική

ικανότητα» της ΕΕ (Bach & Newman, 2008). Ο όρος της «κανονιστικής ικανότητας» νοείται ως η ικανότητα ενός κράτους να αναπτύσσει, να συντονίζει και να εφαρμόζει τους κανόνες της αγοράς. Η ικανότητα αυτή, έχει τουλάχιστον τρεις διαστάσεις: (α) την εμπειρογνωμοσύνη (δηλαδή, την ικανότητα των «υπεύθυνων χάραξης πολιτικής» να εντοπίζουν τις κανονιστικές προκλήσεις, να αναπτύσσουν νομοθετικές λύσεις και να τις εφαρμόζουν), (β) τη συνοχή (δηλαδή, την σαφή διατύπωση των ρυθμίσεων) και (γ) τον έλεγχο εφαρμογής των κανόνων και την επιβολή κυρώσεων σε περίπτωση μη συμμόρφωσης (Bach & Newman, 2008).

Το «Φαινόμενο των Βρυξελλών» («Brussels Effect») είναι ένας όρος που επινοήθηκε από την καθηγήτρια Anu Bradford το 2012 και αναπτύχθηκε περαιτέρω από την ίδια το 2015 και το 2020. Το έργο της Bradford σχετικά με το «Brussels Effect» βασίζεται στις παραπάνω θεωρίες, αλλά επιχειρεί να παράσχει μια πιο ολοκληρωμένη και αναλυτική επεξήγηση για το πώς και γιατί συντελείται αυτός ο «εξευρωπαϊσμός» των κανόνων (Bygrave, 2020). Η Bradford περιγράφει τον όρο «Brussels Effect» ως μια διαδικασία μονομερούς ρυθμιστικής παγκοσμιοποίησης, δηλαδή μια διαδικασία κατά την οποία ένα κράτος είναι σε θέση να εξωτερικεύσει τους νόμους της εκτός των συνόρων του, με αποτέλεσμα την παγκοσμιοποίηση των προτύπων του (Bradford, 2012).

4.1.2 Οι προϋποθέσεις για τη μονομερή ρυθμιστική παγκοσμιοποίηση

Σύμφωνα με την άποψη της Bradford, το «φαινόμενο των Βρυξελλών» δεν είναι το αποτέλεσμα μιας συνειδητής επιβολής των ρυθμιστικών προτύπων της ΕΕ σε κράτη εκτός των συνόρων της. Όπως οι Newman, Bach και πολλοί άλλοι θεωρητικοί, η Bradford εντοπίζει ως κρίσιμη προϋπόθεση για το «φαινόμενο των Βρυξελλών» την ύπαρξη μιας μεγάλης εγχώριας αγοράς, αλλά και την κανονιστική ικανότητα ενός κράτους (Bygrave, 2020). Σε αυτούς τους παράγοντες, προσθέτει τρεις ακόμη προϋποθέσεις.

Πιο συγκεκριμένα, σύμφωνα με τη θεωρία της Bradford, το «φαινόμενο των Βρυξελλών» υλοποιείται αυτόματα, όποτε πληρούνται σωρευτικά πέντε προϋποθέσεις: πρώτον, η επαρκώς μεγάλη αγορά του κράτους, δεύτερον, η κανονιστική ικανότητα του κράτους να δημιουργεί και να επιβάλλει πρότυπα, τρίτον, η προτίμηση του κράτους για αυστηρά πρότυπα, τέταρτον, η στόχευση σε «ανελαστικούς στόχους» (όπως είναι οι καταναλωτές) και πέμπτον, η μη διαχωρισιμότητα της παραγωγής ή της συμπεριφοράς μιας εταιρείας. Η μη διαχωρισιμότητα σημαίνει ότι θα πρέπει να είναι αδύνατο για τις εταιρείες να διαφοροποιήσουν τη συμμόρφωσή τους με το καθορισμένο πρότυπο μεταξύ των δικαιοδοσιών (Bradford 2012 & 2014).

Στην παγκόσμια οικονομία, η ισχύς μίας εσωτερικής αγοράς συσχετίζεται με το σχετικό μέγεθος της. Η ΕΕ αποτελεί μία από τις μεγαλύτερες οικονομίες στον κόσμο με Ακαθάριστο Εγχώριο Προϊόν (ΑΕΠ) σχεδόν 20 τρισεκατομμυρίων δολαρίων, που αποτελείται από μια ενιαία αγορά με 500 εκατομμύρια καταναλωτές[35]. Η ΕΕ έχει το ένα τέταρτο του συνολικού Ακαθάριστου Εθνικού Προϊόντος (ΑΕΠ) των χωρών παγκοσμίως και είναι ο μεγαλύτερος εισαγωγέας αγαθών και υπηρεσιών (Bradford, 2014). Καθίσταται σαφές

[35] CIA WORLD FACTBOOK, European Union, https://www.cia.gov/library/publications/the-worldsfactbook/geos/ee.html (τελευταία προσπέλαση: 22 Απριλίου 2024). The GDP figure is based on purchasing power parity (PPP).

ότι οι Ηνωμένες Πολιτείες, η Κίνα και η Ιαπωνία διαθέτουν επίσης εσωτερικές αγορές αρκετά μεγάλες ώστε να χρησιμοποιούν την πρόσβαση στις αγορές τους ως μοχλό πίεσης. Η οικονομία των ΗΠΑ ξεπερνά τα 21 τρισεκατομμύρια δολάρια[36], σχεδόν το ίδιο μέγεθος με αυτό της ΕΕ, ενώ η Κίνα έχει οικονομία σχεδόν 25 τρισεκατομμυρίων δολαρίων[37] και η Ιαπωνία 5 τρισεκατομμυρίων δολαρίων[38]. Ωστόσο, δεδομένου του μεγέθους της αγοράς της Ευρωπαϊκής Ένωσης, και δεδομένου ότι αυτή αποτελείται σε υψηλό ποσοστό από εύπορους καταναλωτές, ένας σημαντικός αριθμός παραγωγών εξαρτάται από την ικανότητά τους να προμηθεύουν την αγορά της ΕΕ, καθώς ναι μεν μπορούν να εκτρέψουν μέρος των εξαγωγών τους αλλού, αλλά λίγοι παραγωγοί είναι σε θέση να ανακτήσουν τα διαφυγόντα έσοδα από άλλες αγορές (Bradford, 2012).

Το μεγάλο μέγεθος της αγοράς από μόνο του δεν εξηγεί την ικανότητα ενός κράτους να επιβάλλει την ρυθμιστικές προτιμήσεις σε άλλους, αλλά απαιτείται, επιπλέον, το κράτος αυτό να έχει «κανονιστική ικανότητα» (Bach & Newman, 2007). Η «κανονιστική ικανότητα» είναι μια συνειδητή επιλογή ενός κράτους και δεν αποτελεί εγγενές χαρακτηριστικό σε κάθε κράτος, που έχει μεγάλη αγορά. Ένα σημαντικό στοιχείο της «κανονιστικής ικανότητας» είναι η εξουσία του κράτους να εφαρμόζει αποτελεσματικά τους νόμους που υιοθετεί, επιβάλλοντας αυστηρές κυρώσεις σε περίπτωση μη συμμόρφωσης. Μόνο οι δικαιοδοσίες που έχουν την ικανότητα να αποκλείσουν όσες επιχειρήσεις δεν συμμορφώνονται με τα πρότυπά τους, επιβάλλοντας ταυτόχρονα σε αυτές σημαντικό κόστος, μπορούν να επιβάλουν την προσαρμογή των πολιτικών των άλλων κρατών σύμφωνα με τα ρυθμιστικά πρότυπα των δικαιοδοσιών αυτών (Bach & Newman, 2007).

Στην Ευρωπαϊκή Ένωση, το Συμβούλιο της Ευρωπαϊκής Ένωσης, μαζί με το Ευρωπαϊκό Κοινοβούλιο, ασκεί τη νομοθετική εξουσία στην ΕΕ. Το Συμβούλιο λαμβάνει αποφάσεις με απλή ή ειδική πλειοψηφία ή, ανάλογα με το θέμα, ομόφωνα. Η Ευρωπαϊκή Επιτροπή διαθέτει σημαντική ανεξαρτησία εξουσία λήψης αποφάσεων. Προτείνει νομοθεσία και διασφαλίζει ότι οι Κανονισμοί και οι Οδηγίες που εκδίδονται από το Συμβούλιο και το Κοινοβούλιο εφαρμόζονται από τα κράτη μέλη. Εάν ένα μεμονωμένο κράτος μέλος δεν εφαρμόσει ορισμένους Κανονισμούς, η Επιτροπή έχει την εξουσία να εναγάγει το κράτος μέλος που δεν συμμορφώνεται ενώπιον των ευρωπαϊκών δικαστηρίων (Bradford, 2012). Η «κανονιστική ικανότητα» της ΕΕ είναι πιο εκτεταμένη σε τομείς όπως το εμπόριο και την πολιτική ανταγωνισμού, οι οποίοι είναι θεμελιώδεις για την εγκαθίδρυση και την ενίσχυση της ενιαίας αγοράς, ενώ, είναι πιο περιορισμένη σε ευαίσθητους τομείς, όπως η κοινή εξωτερική πολιτική και η πολιτική ασφάλειας, όπου τα κράτη μέλη έχουν διατηρήσει σημαντική εξουσία (Bradford, 2012).

---

[36] CIA WORLD FACTBOOK, United States, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (τελευταία προσπέλαση: 22 Απριλίου 2024). The GDP figure is based on purchasing power parity (PPP).

[37] CIA WORLD FACTBOOK, China, https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html (τελευταία προσπέλαση: 22 Απριλίου 2024). The GDP figure is based on purchasing power parity (PPP).

[38] CIA WORLD FACTBOOK, Japan, https://www.cia.gov/library/publications/the-world-factbook/geos/ja.html (τελευταία προσπέλαση: 22 Απριλίου 2024). The GDP figure is based on purchasing power parity (PPP).

Ένα κράτος, προκειμένου να επιβάλλει τα ρυθμιστικά του πρότυπα σε τρίτα κράτη, πρέπει, επίσης, να έχει την τάση να εκδίδει αυστηρά ρυθμιστικά πρότυπα. Η εγχώρια προτίμηση για αυστηρές ρύθμιση είναι πιθανότερο να συναντάται σε «εύπορα» κράτη (Guasch & Hahn, 1999). Οι πλουσιότερες χώρες μπορούν να αντέξουν σε μεγαλύτερο βαθμό την επιδίωξη της προστασίας των καταναλωτών εις βάρος της κερδοφορίας των επιχειρήσεών τους (Bradford, 2012). Η προτίμηση των φορέων χάραξης πολιτικής της ΕΕ για αυστηρή ρύθμιση αντικατοπτρίζει τη δέσμευσή τους σε μια κοινωνική οικονομία της αγοράς[39] (Bradford, 2012).

Οι αυστηροί εγχώριοι κανονισμοί μπορούν να λειτουργήσουν ως παγκόσμια πρότυπα, μόνο εφόσον οι εν λόγω αυστηροί κανονισμοί δεν μπορούν να παρακαμφθούν με τη μετακίνηση των «ρυθμιστικών στόχων» σε άλλη δικαιοδοσία. Ένα τρίτο κράτος έχει την ικανότητα να παρακάμψει τις αυστηρές ρυθμίσεις που έχει θεσμοθετήσει ένα άλλο κράτος εάν ο «στόχος» μπορεί να αποφευχθεί με απλή μετεγκατάσταση (Bradford, 2012). Η ΕΕ αποφεύγει αυτή την καταστρατήγηση των προτύπων της ρυθμίζοντας κυρίως τις καταναλωτικές αγορές, όπως η ασφάλεια των προϊόντων ή των τροφίμων. Σε αντίθεση με έναν ρυθμιστικό στόχο όπως το κεφάλαιο, το οποίο είναι κινητό, οι καταναλωτές δεν μετακινούνται σε άλλη δικαιοδοσία ως απάντηση σε αυστηρά ρυθμιστικά πρότυπα. Έτσι, εφόσον μια επιχείρηση επιθυμεί να έχει πρόσβαση στους 500 εκατομμύρια καταναλωτές της ΕΕ, θα πρέπει να συμμορφώνεται με τους κανόνες της για την προστασία των καταναλωτών, καθώς αυτοί δεν μπορούν να μετακινηθούν σε δικαιοδοσία όπου υφίστανται χαμηλότερα πρότυπα για τα προϊόντα που κινούνται στην αγορά (Bradford, 2012). Η ανελαστικότητα των καταναλωτών ως «ρυθμιστικών στόχων» μπορεί να αντιπαραβληθεί με το κεφάλαιο, το οποίο είναι κινητικό και σε περίπτωση που, για παράδειγμα, η ΕΕ προσπαθούσε να εναρμονίσει τα φορολογικά επίπεδα σε υπερβολικά υψηλά επίπεδα, ένας αριθμός επιχειρήσεων θα μπορούσε να εγκαταλείψει την δικαιοδοσία της και να μετακινήσει το κεφάλαιό της σε άλλο κράτος. Συνεπώς, η επιλογή της ΕΕ να εστιάσει την προσοχή της στους καταναλωτές αναφορικά με τις ρυθμιστικές της προσπάθειες μέχρι στιγμής, ενίσχυσε περαιτέρω το ρόλο της ως παγκόσμιος ρυθμιστής προτύπων (Bradford, 2012).

Ωστόσο, με την εκπλήρωση αυτών των προϋποθέσεων δεν συνεπάγεται ότι τα αυστηρό πρότυπα θα υιοθετηθούν παγκοσμίως. Το «Brussels Effect» ενεργοποιείται μόνο, όταν η επιχείρηση τρίτης χώρας, αφού προσαρμόσει τα προϊόντα του ή τις επιχειρηματικές πρακτικές του ώστε να συμμορφώνονται με τα αυστηρά πρότυπα, αποφασίζει να εφαρμόσει οικειοθελώς αυτό το πρότυπο στα προϊόντα ή τη συμπεριφορά του παγκοσμίως (Bradford, 2012). Μία επιχείρηση έχει κίνητρο να υιοθετήσει ένα αυστηρό πρότυπο παγκοσμίως, όταν η παραγωγή ή η συμπεριφορά του δεν είναι διαχωρίσιμη σε διάφορες αγορές. Η υιοθέτηση ενός ενιαίου προτύπου επιτρέπει σε μια επιχείρηση να διατηρήσει μία ενιαία παραγωγική

[39] Η δέσμευση της ΕΕ για την κοινωνική οικονομία της αγοράς αναφέρεται ρητά ως κοινός στόχος για την Ευρώπη, ο οποίος προστίθεται στο άρθρο 1 της νέας Συνθήκης της Λισαβόνας, «Η Ένωση εργάζεται για τη βιώσιμη ανάπτυξη της Ευρώπης με γνώμονα την ισόρροπη οικονομική ανάπτυξη και τη σταθερότητα των τιμών, την άκρως ανταγωνιστική κοινωνική οικονομία της αγοράς, με στόχο την πλήρη απασχόληση και την κοινωνική πρόοδο, και το υψηλό επίπεδο προστασίας και βελτίωσης της ποιότητας του περιβάλλοντος.».

διαδικασία, που είναι λιγότερο δαπανηρή από το να προσαρμόζει την παραγωγή της για να ανταποκρίνεται σε αποκλίνοντα ρυθμιστικά πρότυπα και διευκολύνει τη διατήρηση ενός ενιαίου παγκόσμιου εμπορικού σήματος (Vogel, 2012).

Συνεπώς, το φαινόμενο των Βρυξελλών προκύπτει από τη μη διαχωρισιμότητα της παραγωγής μιας επιχείρησης ή της συμπεριφοράς της. Η μη διαχωρισιμότητα της παραγωγής ή της συμπεριφοράς μιας εταιρείας εμφανίζεται σε τρεις περιπτώσεις: η νομική μη-διαχωρισιμότητα, η τεχνική μη-διαχωρισιμότητα και η οικονομική μη-διαχωρισιμότητα. Η νομική μη-διαχωρισιμότητα, μπορεί να παρατηρηθεί στις παγκόσμιες συγχωνεύσεις, οι οποίες δεν μπορούν να πραγματοποιηθούν σε επίπεδο δικαιοδοσίας ανά δικαιοδοσία, αλλά η πιο αυστηρή αντιμονοπωλιακή δικαιοδοσία καθορίζει την τύχη της συναλλαγής παγκοσμίως (Bradford, 2012). Η αρχή της «τεχνικής μη διαχωρισιμότητας» συχνά εφαρμόζεται για τη ρύθμιση της ιδιωτικής ζωής. Για παράδειγμα, η ΕΕ υποχρεώνει τις εταιρείες, όπως τη Google να τροποποιήσουν την αποθήκευση δεδομένων και άλλες επιχειρηματικές πρακτικές τους ώστε να συμμορφωθούν με τα ευρωπαϊκά πρότυπα προστασίας της ιδιωτικής ζωής. Στην περίπτωση αυτή, η επιχείρηση (εν προκειμένω η Google) αδυνατεί να απομονώσει τη συλλογή δεδομένων της για την ΕΕ για τεχνικούς λόγους, και αναγκάζεται να προσαρμόσει τις παγκόσμιες δραστηριότητές της στα πιο απαιτητικά πρότυπα της ΕΕ (Bradford, 2014). Τέλος, η «οικονομική μη διαχωρισιμότητα» καταδεικνύεται στις αντιδράσεις των συμμετεχόντων στην αγορά στις αποφάσεις της ΕΕ για την υγεία, το περιβάλλον και στα πρότυπα προϊόντων. Ένα ενδεικτικό παράδειγμα είναι η ευρωπαϊκή ρύθμιση για τα χημικά προϊόντα, η οποία ισχύει για όλες τις εταιρείες που επιδιώκουν να εισέλθουν στην αγορά της ΕΕ. Πολυάριθμοι κατασκευαστές των ΗΠΑ, οι οποίοι θεωρούσαν υπερβολικά δαπανηρή την ανάπτυξη διαφορετικών προϊόντων για διαφορετικές αγορές καταναλωτών, επιλέγουν να συμμορφώσουν ολόκληρη την παγκόσμια παραγωγή χημικών προϊόντων τους με το πρότυπο της ΕΕ (Bradford, 2012).

Στην περίπτωση της νομοθεσίας της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων, φαίνεται να πληρούνται οι πέντε προϋποθέσεις. Αρχικά, όπως αναφέρθηκε ανωτέρω η Ευρωπαϊκή Ένωση έχει μεγάλο μέγεθος αγοράς. Δεύτερον, η Ευρωπαϊκή Ένωση έχει σημαντική «κανονιστική ικανότητα» όσον αφορά την προστασία προσωπικών δεδομένων, έχοντας υιοθετήσει ένα σαφές και ολοκληρωμένο νομοθετικό πλαίσιο, ενιαίο για όλα τα κράτη μέλη και έχοντας τη δυνατότητα επιβολής των κανόνων αυτών μέσω των αρμόδιων αρχών της Ένωσης και των κρατών μελών (Schwartz, 2019). Τρίτον, οι κανόνες της ΕΕ για την προστασία των δεδομένων, ιδίως ο GDPR, θεωρούνται γενικά αυστηροί. Τέταρτον, αν και ο GDPR δεν στοχεύει στους καταναλωτές, στοχεύει σε μια έννοια που πλησιάζει πολύ: τα υποκείμενα των δεδομένων (Gunst & Ferdi de Ville, 2021). Πέμπτον, η Bradford υποστηρίζει ότι η συμμόρφωση με κανόνες προστασίας δεδομένων όπως ο GDPR είναι αδιαίρετη με την τεχνική έννοια. Υποστηρίζει ότι είναι δύσκολο για τις εταιρείες να εκτιμήσουν ποιος νόμος περί προστασίας δεδομένων της ποιας δικαιοδοσίας εφαρμόζεται σε ένα συγκεκριμένο σύνολο δεδομένων. Ως εκ τούτου, είναι ασφαλέστερο και πιο πρακτικό για μια εταιρεία να συμμορφώνεται με τον αυστηρότερο νόμο περί προστασίας δεδομένων, προκειμένου να μην παραβιάσει τον εν λόγω νόμο κατηγοριοποιώντας εσφαλμένα ορισμένα δεδομένα σε λιγότερο αυστηρό νόμο (Bradford, 2012).

Η ανάλυση του «Brussels Effect» από την Bradford είναι σε μεγάλο βαθμό τεκμηριωμένη, ωστόσο, ορισμένες πτυχές της δεν συνάδουν πλήρως με τον τρόπο με τον οποίο οι κανόνες της ΕΕ για την προστασία των δεδομένων έχουν εξαπλωθεί σε ολόκληρο τον κόσμο (Bygrave, 2020). Πρώτον, ο χαρακτηρισμός του φαινομένου των Βρυξελλών ως «μονομερούς» διαδικασίας υποβαθμίζει τη διμερή και αμφίδρομη φύση της σχέσης μεταξύ της ΕΕ και άλλων κρατών στο πεδίο της προστασίας των δεδομένων. Η Ευρωπαϊκή Ένωση δεν άσκησε μονομερή εξουσία, επιβάλλοντας τα ρυθμιστικά της πρότυπα σε τρίτα κράτη, αλλά αντιθέτως, επέτρεψε κάποια ευελιξία και διαπραγμάτευση ιδίως κατά την αξιολόγηση της επάρκειας των τρίτων κρατών αναφορικά με τη νομοθεσία για την προστασία των δεδομένων (Schwartz, 2019). Δεύτερον, όπως εύστοχα παρατηρεί ο Schwartz, η ΕΕ δεν «επιβλήθηκε» στα άλλα κράτη αποκλειστικά λόγω της ισχύς της αγοράς της, αλλά και λόγω της ισχύς της ιδεολογίας της (Schwartz, 2013). Το ρυθμιστικό μοντέλο που έχει επιλέξει η ΕΕ, βασίζεται σε γενικές αρχές που προσφέρουν υψηλά πρότυπα προστασίας δεδομένων και είναι σχετικά απλό, προσιτό, ελκυστικό και εύκολο να υιοθετηθεί από τρίτα κράτη (Schwartz, 2013 & Bradford, 2019).

4.2 Οι εκφάνσεις του «Brussels Effect» στην προστασία προσωπικών δεδομένων

4.2.1 Το de facto «Brussels effect»

Σύμφωνα με τη θεωρία της Bradford, υπάρχουν δύο εκφάνσεις του «φαινομένου των Βρυξελλών»: το de facto και το de jure «φαινόμενο των Βρυξελλών». Το de facto «φαινόμενο των Βρυξελλών» εμφανίζεται όταν οι εταιρείες συμμορφώνονται οικειωθελώς με τα πρότυπα της Ευρωπαϊκής Ένωσης στην παγκόσμια αλυσίδα παραγωγής τους (Bradford, 2012).

Το de facto «φαινόμενο των Βρυξελλών» στον τομέα προσωπικών δεδομένων, ενισχύεται από τις διατάξεις του GDPR σχετικά με τη διαβίβαση δεδομένων σε τρίτες χώρες, που αναγκάζει τις εταιρείες να χρησιμοποιούν μηχανισμούς όπως τους «δεσμευτικούς εταιρικούς κανόνες» και τις «τυποποιημένες συμβατικές ρήτρες», όταν διαβιβάζουν δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα. Αυτοί οι μηχανισμοί καταλήγουν ουσιαστικά στο ότι μια εταιρεία υποβάλλει οικειοθελώς τον εαυτό της σε πτυχές του GDPR στην εμπλεκόμενη τρίτη χώρα (η οποία αντιστοιχεί στο de facto φαινόμενο των Βρυξελλών (Gunst & Ferdi de Ville, 2021).

Δεδομένου ότι ο GDPR εφαρμόζεται σε όλες τις επιχειρήσεις, που προσφέρουν αγαθά ή υπηρεσίες στην ΕΕ ή παρακολουθούν τις δραστηριότητες των πολιτών της ΕΕ, ανεξαρτήτως τοποθεσίας, το πεδίο εφαρμογής του GDPR, δεν περιορίζεται στα γεωγραφικά όρια της ΕΕ, αλλά εφαρμόζεται και σε επιχειρήσεις τρίτων κρατών όταν ισχύουν οι ανωτέρω προϋποθέσεις. Ως εκ τούτου, όλες οι εταιρείες που εδρεύουν σε τρίτες χώρες θα μπορούσαν είτε να συμμορφωθούν με τον GDPR ή να παύσουν να προσφέρουν πωλήσεις και υπηρεσίες στους καταναλωτές της ΕΕ. Η επιλογή αυτή δεν θεωρείται μια ελεύθερη επιλογή, καθώς δεν υπάρχει πραγματική εναλλακτική λύση για τις περισσότερες εταιρείες, δεδομένης της σημαντικότητας της αγοράς της ΕΕ (Rustad & Koenig, 2019).

Στο πλαίσιο αυτό, εταιρείες-κολοσσοί στον τομέα της τεχνολογίας δεσμεύονται να αλλάξουν τις πολιτικές τους προκειμένου να επιτύχουν τη συμμόρφωσή τους με την προστασία της ιδιωτικής ζωής των δεδομένων του GDPR (Rustad & Koenig, 2019). Ωστόσο,

πολλές φορές οι επιχειρήσεις δεν περιορίζουν την εφαρμογή των πολιτικών, που είναι σύμφωνοι με τον GDPR μόνο στην ΕΕ, αλλά επεκτείνουν τις πολιτικές αυτές και στους καταναλωτές εκτός ΕΕ Όπως αναφέρθηκε ανωτέρω, είναι πιο αποδοτικό από πλευράς κόστους για μια πολυεθνική εταιρεία να υιοθετεί ένα ενιαίο νομικό πρότυπο αντί να συμμορφώνεται με πολλαπλά αποκλίνοντα πρότυπα που ενίοτε συγκρούονται.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση του Facebook αναφορικά με την προστασία των προσωπικών δεδομένων. Το Μάρτιο του 2018, κατέστη δημοσίως γνωστό το σκάνδαλο της Cambridge Analytica, μετά από μαρτυρίες πρώην υπαλλήλων της Cambridge Analytica ότι υπήρξαν παραβιάσεις προσωπικών δεδομένων Ευρωπαίων πολιτών (Cadwalladr & Graham-Harrison, 2018). Ειδικότερα, αποκαλύφθηκε ότι η Cambridge Analytica, μία εταιρεία ανάλυσης δεδομένων, εκμεταλλεύτηκε τα δεδομένα, στα οποία απέκτησε πρόσβαση μέσω του Facebook, προκειμένου να δημιουργήσει στοχευμένες πολιτικές διαφημιστικές εκστρατείες, επηρεάζοντας τις εκλογές και την κοινή γνώμη μέσω προσαρμοσμένων μηνυμάτων.

Τον Απρίλιο του 2018, με αφορμή το σκάνδαλο της ο διευθύνων σύμβουλος του Facebook, Mark Zuckerberg, κατέθεσε στην Επιτροπή Δικαιοσύνης της Γερουσίας και στην Επιτροπή Εμπορίου, Επιστήμης και Μεταφορών και απαντώντας σε ερωτήσεις σχετικά με το Facebook για τις πρακτικές απορρήτου δεδομένων, ανέλαβε προσωπική ευθύνη για την ανεπαρκή προστασία του απορρήτου των χρηστών του Facebook (Rustad & Koenig, 2019). Ήδη πριν την κατάθεσή του, ο Zuckerberg υποσχέθηκε να επεκτείνει την προστασία των προσωπικών δεδομένων που παρέχει ο GDPR σε όλους τους χρήστες του Facebook παγκοσμίως (Rustad & Koenig, 2019). Τον Απρίλιο του 2018, το Facebook ανακοίνωσε ότι θα υιοθετήσει ομοιόμορφα πρακτικές απορρήτου προκειμένου να συμμορφωθεί με τον GDPR και εκτός Ευρωπαϊκής Ένωσης[40].

Το Facebook έχει μια γενική «πολιτική δεδομένων». Ωστόσο, για τις ΗΠΑ ισχύει διαφορετική έκδοση αυτής της πολιτικής από ό,τι για την ΕΕ. Ενώ ορισμένες έννοιες του GDPR περιλαμβάνονται στις πολιτικές απορρήτου του Facebook, είναι υπερβολικό να υποστηριχθεί, ότι τα ευρωπαϊκά πρότυπα απορρήτου έχουν επεκταθεί σε όλους τους χρήστες της εταιρείας παγκοσμίως. Το πιο προφανές παράδειγμα της επέκτασης του GDPR σε όλους χρήστες του Facebook είναι η συμπερίληψη στην πολιτική αρκετών δικαιωμάτων του υποκειμένου των δεδομένων και της αρχής του περιορισμού της αποθήκευσης. Ωστόσο, υπάρχουν αρκετές διαφοροποιήσεις για τους χρήστες εκτός ΕΕ, ιδίως αναφορικά με τα ευαίσθητα προσωπικά δεδομένα και τη λήψη ρητής συγκατάθεσης (Gunst & Ferdi de Ville, 2021).

Η Google περιλαμβάνει αρκετές έννοιες του GDPR στις πολιτικές της για τους χρήστες εκτός ΕΕ. Για παράδειγμα, ο ορισμός της Google για τις προσωπικές πληροφορίες είναι αρκετά συνεπής με τον ορισμό των προσωπικών δεδομένων στον GDPR[41]. Η Google περιλαμβάνει επίσης αρκετές αρχές προστασίας δεδομένων στους χρήστες εκτός ΕΕ.

[40] Facebook's Commitment to Data Protection and Privacy in Compliance with the GDPR, FACEBOOK, διαθέσιμο εδώ https://www.facebook.com/business/news/facebookscommitm , (τελευταία προσπέλαση: 22 Απριλίου 2024)

[41] Google, Privacy Policy, διαθέσιμο εδώ https://policies.google.com/privacy/archive/20180525?hl=en-US (τελευταία προσπέλαση: 22 Απριλίου 2024).

Ειδικότερα, όσον αφορά την αρχή της ασφάλειας των δεδομένων, αντιγράφει σε μεγάλο βαθμό τις σχετικές διατάξεις του GDPR. Ωστόσο, παρόλο που η πολιτική απορρήτου της Google έχει παγκόσμια εφαρμογή, αυτό υπονομεύεται από την παρουσία μίας ενότητας «ευρωπαϊκές απαιτήσεις» σε αυτήν. Η εν λόγω ενότητα περιλαμβάνει το δικαίωμα περιορισμού της επεξεργασίας και το δικαίωμα εναντίωσης, τα οποία, επομένως, δεν είναι διαθέσιμα στους χρήστες της Google εκτός ΕΕ. Η ενότητα περιλαμβάνει, επιπλέον, πληροφορίες σχετικά με τις νομικές βάσεις (όπως η συγκατάθεση) που χρησιμοποιεί η Google για την επεξεργασία των προσωπικών δεδομένων των χρηστών της στην ΕΕ (Gunst & Ferdi de Ville, 2021).

Τέλος, και η Microsoft έχει δεσμευτεί να συμμορφωθεί με τον GDPR σε διεθνές επίπεδο. Πιο συγκεκριμένα, η εταιρία προέβη σε μία ολοσέλιδη διαφήμιση στην εφημερίδα της New York Times, υποστηρίζοντας ότι ο GDPR θα της έδινε ανταγωνιστικό πλεονέκτημα στην εμπιστοσύνη των καταναλωτών[42]. Τον Μάιο του 2018, η Microsoft ανακοίνωσε ότι επρόκειτο να επεκτείνει τα δικαιώματα που παρέχονται από τον GDPR σε όλους τους καταναλωτές παγκοσμίως[43] (Rustad & Koenig, 2019). Πράγματι, η Microsoft έχει υιοθετήσει μία ενιαία πολιτική προστασίας δεδομένων, έχοντας ωστόσο και μία ξεχωριστή ενότητα για τους χρήστες που κατοικούν στις ΗΠΑ[44].

4.2.2 To de iure «Brussels effect»

Το de jure «φαινόμενο των Βρυξελλών» εμφανίζεται όταν οι δικαιοδοσίες εκτός Ευρωπαϊκής Ένωσης ενσωματώνουν τα πρότυπα της ΕΕ, υιοθετώντας αντίστοιχες νομοθεσίες. Η Bradford θεωρεί ότι το de jure «φαινόμενο των Βρυξελλών» συμβαίνει σε μεγάλο βαθμό επειδή οι εταιρείες που επηρεάζονται από το de facto «φαινόμενο των Βρυξελλών» ασκούν πίεση στις εγχώριες κυβερνήσεις τους να υιοθετήσουν τα πρότυπα της ΕΕ, προκειμένου να εξισωθούν οι όροι ανταγωνισμού έναντι του εγχώριου -μη επηρεαζόμενου- ανταγωνιστή τους. Αυτό σημαίνει ότι το de jure φαινόμενο μπορεί να χαρακτηριστεί ως ένα είδος λογικής συνέχειας του de facto «φαινομένου των Βρυξελλών» (Bradford, 2012).

Το de jure «φαινόμενο των Βρυξελλών» ενισχύεται από τις διατάξεις του GDPR αναφορικά με την απόφαση επάρκειας. Για να λάβει απόφαση επάρκειας, μια τρίτη χώρα πρέπει να προσαρμόσει το δικό της πλαίσιο προστασίας δεδομένων κατά τρόπο ώστε να είναι «επαρκές». Για να εξασφαλιστεί η ελεύθερη ροή δεδομένων προσωπικού χαρακτήρα, οι αποφάσεις επάρκειας είναι ιδιαίτερα πολύτιμες για κάθε τρίτη χώρα, δίνοντας έτσι κίνητρο σε τρίτες χώρες να μιμηθούν τον GDPR (Gunst & Ferdi de Ville, 2021).

---

[42] Microsoft, There's a Data Crackdown Coming. Why It's Good for Customers and Business, N.Y. TIMES, διαθέσιμο εδώ https://www.nytimes.com/paidpost/microsoft/theres-a-data-crackdown-coming.html (τελευταία προσπέλαση: 22 Απριλίου 2024).

[43] Microsoft, Microsoft's commitment to GDPR, privacy and putting customers in control of their own data, διαθέσιμο εδώ https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ (τελευταία προσπέλαση: 22 Απριλίου 2024).

[44] Microsoft, Privacy Statement, https://privacy.microsoft.com/el-GR/privacystatement#maincaliforniaconsumerprivacyactmodule (τελευταία προσπέλαση: 22 Απριλίου 2024)

Ιδιαίτερο ενδιαφέρον παρουσιάζει η επίδραση της ΕΕ στη νομοθεσία της Ιαπωνίας για την προστασία προσωπικών δεδομένων. Στις 23 Ιανουαρίου 2019, η ΕΕ και η Ιαπωνία κατέληξαν σε αμοιβαία συμφωνία επάρκειας, η οποία επιτρέπει την ελεύθερη ροή δεδομένων προσωπικού χαρακτήρα μεταξύ των δύο οικονομιών, μετά από εκτεταμένες διαπραγματεύσεις που διήρκησαν δύο έτη. Κατά την επισκόπηση της νομοθεσίας της Ιαπωνίας για την προστασία της ιδιωτικής ζωής το 2014, ο Greenleaf τη χαρακτήρισε ως «την ψευδαίσθηση της προστασίας» (Greenleaf, 2014). Ειδικότερα, άσκησε κριτική στον ιαπωνικό νόμο περί προστασίας των δεδομένων για το περιορισμένο πεδίο εφαρμογής του στον ιδιωτικό τομέα, την απουσία διατάξεων για τις ευαίσθητες πληροφορίες και την έλλειψη περιορισμού των εξαγωγών δεδομένων (Greenleaf, 2014). Ωστόσο, από το 2015 και μετά επήλθαν βασικές αλλαγές με τις εκτεταμένες τροποποιήσεις του ιαπωνικού νόμου για την προστασία των προσωπικών δεδομένων (APPI). Σε αυτές περιλαμβάνονται ένας διευρυμένος ορισμός των ευαίσθητων δεδομένων, περισσότερα ατομικά δικαιώματα, αυστηρότεροι περιορισμοί στη διαβίβαση των προσωπικών δεδομένων και ενισχυμένες εξουσίες επιβολής της ιαπωνικής αρχής προστασίας δεδομένων, της Επιτροπής Προστασίας Προσωπικών Πληροφοριών (Personal Information Protection Commission - PPC). Οι τροποποιήσεις του APPI άλλαξαν την ιαπωνική νομοθεσία κατά τρόπο που την έφερε σημαντικά πιο κοντά στο πρότυπο της ΕΕ (Schwartz, 2019).

Η θεωρία «του φαινομένου των Βρυξελλών» της Anu Bradford δεν αντικατοπτρίζεται πλήρως στο παράδειγμα της Ιαπωνίας. Η διαδικασία υιοθέτησης νομοθεσίας αντίστοιχης με τα πρότυπα της ΕΕ, δεν ήταν ούτε μονομερής ούτε αποτέλεσμα του de facto φαινομένου των Βρυξελλών. Αντιθέτως, η Ιαπωνία επέλεξε συνειδητά ένα σύστημα παρόμοιο και συμβατό με τη νομοθεσία της ΕΕ για την προστασία των δεδομένων. Καθίσταται σαφές ότι καθοριστικό παράγοντα αποτέλεσε το οικονομικό συμφέρον της χώρας, σύμφωνα με την κρίση της σχετικά με τα πλεονεκτήματα των ανταγωνιστικών ρυθμιστικών συστημάτων για την προστασία της ιδιωτικής ζωής των δεδομένων (Schwartz, 2019).

Εν συνεχεία, παρά το γεγονός ότι στις ΗΠΑ δεν υφίσταται ένα ενιαίο και ολοκληρωμένο νομοθετικό πλαίσιο για την προστασία προσωπικών δεδομένων, σε επίπεδο Πολιτειών υπάρχουν νομοθετικές επιλογές, που προσιδιάζουν στον GDPR. Σημαντικότερο παράδειγμα αποτελεί η Καλιφόρνια, όπου εφαρμόζεται ο California Consumer Privacy Act of 2018 (CCPA), όπως έχει τροποποιηθεί με τον California Privacy Rights Act (CPRA). Το νομοθετικό αυτό πλαίσιο, παρά το γεγονός ότι διαφέρει σε ορισμένα σημεία με τον GDPR, όπως αναλύθηκε ειδικότερα ανωτέρω, παρέχει επαρκές επίπεδο προστασίας και σε μεγάλο βαθμό όμοιο με αυτό που διασφαλίζει ο GDPR. Ειδικότερα, ο CCPA υιοθετεί ένα διευρυμένο εννοιολογικό περιεχόμενο των προσωπικών πληροφοριών, αντίστοιχο με αυτό των προσωπικών δεδομένων, ενώ και στα δύο νομοθετήματα δίνεται ιδιάζουσα έμφαση στα ατομικά δικαιώματα των καταναλωτών (Field, 2020). Η Καλιφόρνια έχει αποτελέσει παράδειγμα και για άλλες Πολιτείες, οι οποίες έχουν εισαγάγει νομοθεσίες που ενσωματώνουν επίσης ορισμένες πτυχές της πολιτικής της ΕΕ (Field, 2020). Ο λόγος για τον οποίο εξαπλώθηκε ο CCPA, είναι αντίστοιχος με το λόγο που εξαπλώθηκε ο GDPR. Το τεράστιο μέγεθος της Πολιτείας, σε συνδυασμό με την εύρωστη οικονομία της, δίνουν στην Καλιφόρνια σημαντικό πλεονέκτημα στην ενθάρρυνση μεγάλων εταιρειών να υιοθετήσουν τους κανονισμούς της σε εθνικό επίπεδο (Rustad & Koenig, 2019).

Εξάλλου, η Κίνα, στις 20 Αυγούστου 2021 ενέκρινε τον Personal Information Protection Law (PIPL) και την 1η Νοεμβρίου του ίδιου έτους, ο κανονισμός τέθηκε σε ισχύ. Ο PIPL αποτελεί την πρώτη ολοκληρωμένη νομοθεσία για την προστασία των δεδομένων και την ιδιωτικότητα των δεδομένων στην Κίνα[45]. Ωστόσο, σε αντίθεση με την Ευρώπη, που εστιάζει στα ατομικά δικαιώματα, η Κίνα έχει ως κύριο μέλημά της την προστασία των προσωπικών πληροφοριών των Κινέζων πολιτών από ξένες εταιρείες και κράτη (Moreira, 2023). Η κινέζικη κυβέρνηση, ευθυγραμμίζοντας τον εθνικό της νόμο περί προστασίας δεδομένων με τον GDPR, ενισχύει τον έλεγχο και την παρακολούθηση των πολιτών της και του ψηφιακού οικονομικού της τομέα (Daniel, 2022). Ως εκ τούτου, το γεγονός ότι ο GDPR παρέχει μια πολύ αυστηρή νομοθεσία με υψηλό επίπεδο κυβερνητικού ελέγχου τον καθιστά κατάλληλο για το κινεζικό σύστημα (Bradford, 2020). Παράλληλα, το γεγονός ότι υπήρξε μια σειρά από παραβιάσεις δεδομένων,, όπου χάθηκαν οι προσωπικές πληροφορίες εκατομμυρίων πολιτών της Κίνας, ενθάρρυνε την κινεζική κυβέρνηση να εφαρμόσει έναν νόμο παρόμοιο με τον GDPR (Moreira, 2023).

Αντιστοίχως, η Τουρκία μετά την υπογραφή της Σύμβασης 108 του Συμβουλίου της Ευρώπης, θέσπισε το Νόμο 6698 για την προστασία των προσωπικών δεδομένων τον Απρίλιο του 2016, ενώ λίγους μήνες αργότερα επικύρωσε και τη Σύμβαση 108 και λίγο αργότερα και το Πρόσθετο Πρωτόκολλο. Η τουρκική Αρχή Προστασίας Προσωπικών Δεδομένων ιδρύθηκε τον Ιανουάριο του 2017. Ο νόμος της Τουρκίας βασίζεται στην ενωσιακή οδηγία 95/46, έχοντας λίγες αλλά βασικές διαφορές με τον GDPR, ιδίως όσον αφορά τη νομιμότητα της επεξεργασίας και τη διασυνοριακή διαβίβαση δεδομένων προσωπικού χαρακτήρα (Kinikoglu, 2023).

Συνοψίζοντας, σύμφωνα με τη θεωρία της Bradford, η διάδοση της νομοθεσίας της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων, εντοπίζεται με δύο εκφάνσεις, το de facto και το de jure φαινόμενο των Βρυξελλών. Το de facto φαινόμενο των Βρυξελλών εμφανίζεται όταν οι εταιρείες συμμορφώνονται οικειωθελώς με τα πρότυπα της Ευρωπαϊκής Ένωσης στην παγκόσμια αλυσίδα παραγωγής τους, ενώ το de jure φαινόμενο των Βρυξελλών εμφανίζεται ως αναγκαίο επακόλουθο του de facto φαινομένου, όταν οι δικαιοδοσίες εκτός Ευρωπαϊκής Ένωσης ενσωματώνουν τα πρότυπα της ΕΕ στα δικά τους νομικά πλαίσια, υιοθετώντας αντίστοιχες νομοθεσίες. Το φαινόμενο αυτό εξηγείτε αρχικά από το μέγεθος της αγοράς της Ευρωπαϊκής Ένωσης σε συνδυασμό με τη σημαντική «κανονιστικά ικανότητα» της, έχοντας υιοθετήσει ένα αυστηρό νομοθετικό πλαίσιο, ενιαίο για όλα τα κράτη μέλη και έχοντας τη δυνατότητα επιβολής των κανόνων αυτών μέσω των αρμόδιων αρχών της Ένωσης και των κρατών μελών. Ιδιαίτερη σημασία παρουσιάζει το γεγονός ότι η συμμόρφωση με τους κανόνες προστασίας δεδομένων του GDPR είναι αδιαίρετη με την τεχνική έννοια και ως εκ τούτου, είναι δύσκολο για τις εταιρείες να εφαρμόζουν διαφορετική νομοθεσία για κάθε δικαιοδοσία. Ως εκ τούτου, πολλές εταιρείες που εδρεύουν εκτός ΕΕ, έχουν υιοθετήσει παγκοσμίως πρακτικές που συμφωνούν με τις διατάξεις του GDPR, ενώ αντίστοιχα πολλά κράτη έχουν υιοθετήσει αντίστοιχες νομοθεσίες.

[45] Data Guidance, China - Data Protection Overview | Guidance Note | DataGuidance (τελευταία προσπέλαση: 9 Ιουνίου 2024)

5. Η διασυνοριακή ροή προσωπικών δεδομένων

Παράλληλα με την ανάπτυξη του Διαδικτύου, κατέστη εφικτή η διασυνοριακή ροή δεδομένων, δηλαδή η μεταφορά προσωπικών δεδομένων εκτός των εθνικών συνόρων (OECD, 2013). Οι άνθρωποι, οι επιχειρήσεις και οι κυβερνήσεις απέκτησαν τη δυνατότητα να αλλάξουν τον τρόπο με τον οποίο συλλέγονται, μοιράζονται και χρησιμοποιούνται τα δεδομένα. Η αξιοποίηση των διασυνοριακών ροών δεδομένων έχει, με τη σειρά της, αυξήσει την οικονομική αποτελεσματικότητα και την παραγωγικότητα, αυξάνοντας την ευημερία και το βιοτικό επίπεδο παγκοσμίως (Kuner, 2011). Ωστόσο, η αυξανόμενη ροή δεδομένων, έχει προξενήσει ανησυχίες, ιδίως όσον αφορά το απόρρητο και την προστασία των προσωπικών δεδομένων, που διαφέρουν από κράτος σε κράτος (OECD, 2022). Για το λόγο αυτό, σημειώθηκαν σημαντικές πρωτοβουλίες από περιφερειακά όργανα, που αποτέλεσαν τον βασικό μοχλό για τη ρύθμιση της διασυνοριακής ροή των δεδομένων και θα αναλυθούν κατωτέρω.

5.1 Το ρυθμιστικό πλαίσιο

5.1.1 Οι Κατευθυντήριες Γραμμές του ΟΟΣΑ για την Προστασία της Ιδιωτικότητας και τις Διασυνοριακές Ροές Προσωπικών Δεδομένων

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ, Organisation for Economic Co-operation and Development - OECD), που δημιουργήθηκε το 1948 είναι ένα διεθνής οργανισμός των ανεπτυγμένων χωρών που υποστηρίζουν τις αρχές της αντιπροσωπευτικής δημοκρατίας και της οικονομίας της ελεύθερης αγοράς. ΟΟΣΑ, αποτελείται από 38 χώρες-μέλη[46], μεταξύ των οποίων περιλαμβάνονται η Αυστραλία, οι ΗΠΑ, ο Καναδάς, οι χώρες της Ευρωπαϊκής Ένωσης, η Ιαπωνία, το Ηνωμένο Βασίλειο, το Ισραήλ, το Μεξικό, η Τουρκία και η Νότια Κορέα.

Οι Κατευθυντήριες Γραμμές του ΟΟΣΑ για την Προστασία της Ιδιωτικότητας και τις Διασυνοριακές Ροές Προσωπικών Δεδομένων δημοσιεύθηκαν αρχικά το 1980 και αναθεωρήθηκαν το 2013. Οι κατευθυντήριες οδηγίες μπορούν να ακολουθηθούν από οποιαδήποτε χώρα, όχι μόνο από τα μέλη του ΟΟΣΑ. Τα περισσότερα μέλη έχουν ήδη εφαρμόσει ολοκληρωμένη νομοθεσία για την προστασία των δεδομένων, με μοναδική εξαίρεση τις Ηνωμένες Πολιτείες Αμερικής, που δεν έχει υιοθετήσει ακόμη έναν ενιαίο ολοκληρωμένο νόμο (UNCTAD, 2016).

Οι Κατευθυντήριες Γραμμές καθορίζουν δύο τρόπους με τους οποίους τα δεδομένα μπορούν να διαβιβαστούν διασυνοριακά. Ο ένας από αυτούς αντικατοπτρίζει την προσέγγιση της λογοδοσίας, όπου ο υπεύθυνος επεξεργασίας δεδομένων παραμένει υπόλογος για τα δεδομένα προσωπικού χαρακτήρα που βρίσκονται υπό τον έλεγχό του, ανεξάρτητα από τον τόπο αποθήκευσης των δεδομένων. Η άλλη προσέγγιση επιτρέπει τη διαβίβαση δεδομένων σε τρίτη χώρα που τηρεί ουσιαστικά τις κατευθυντήριες γραμμές ή εφόσον υπάρχουν επαρκείς εγγυήσεις, οι οποίες περιλαμβάνουν μηχανισμούς που εξασφαλίζουν τη συνεχή προστασία σύμφωνα με τις κατευθυντήριες γραμμές.

[46] Οι χώρες-μέλη του Ο.Ο.Σ.Α. στο https://www.oecd.org/about/members-and-partners/ (τελευταία προσπέλαση: 17 Απριλίου 2024)

Σύμφωνα με τη συμπληρωματική αιτιολογική έκθεση των κατευθυντήριων γραμμών για την προστασία της ιδιωτικής ζωής, οι δύο αυτές αρχές σχετικά με τη διασυνοριακή διαβίβαση δεδομένων υφίστανται ανεξάρτητα η μία από την άλλη (OECD, 2013). Οι δύο αυτές προσεγγίσεις αντικατοπτρίζουν τις διαφορετικές προσεγγίσεις μεταξύ των μελών του ΟΟΣΑ όσον αφορά τις διασυνοριακές διαβιβάσεις, από τη μία πλευρά, την προσέγγιση της ΕΕ και του GDPR, οι οποίες περιορίζουν τις διαβιβάσεις σε χώρες που παρέχουν επαρκή προστασία, και από την άλλη πλευρά, την προσέγγιση της APEC και του CBPR, που επιτρέπει τις διαβιβάσεις δεδομένων και καθιστά τον υπεύθυνο επεξεργασίας υπεύθυνο για τυχόν παραβιάσεις των εν λόγω δεδομένων που προκύπτουν για τη χρήση τους από τρίτους σε άλλες χώρες (Mattoo & Meltzer, 2018).

Η πρωτοβουλία αυτή του ΟΟΣΑ για την προστασία της ιδιωτικής ζωής έχει σημαντικά θετικά σημεία. Κατά πρώτον, οι κατευθυντήριες γραμμές εστιάζουν στην επίτευξη ισορροπίας μεταξύ της πρόσβασης στα δεδομένα και της χρήσης αυτών από τις επιχειρήσεις και τις διοικητικές αρχές και της προστασίας των δεδομένων. Εξάλλου, είναι αξιοσημείωτο ότι έχουν λάβει ευρεία υποστήριξη από χώρες που ακολουθούν διαφορετικές μεταξύ τους προσεγγίσεις και ως εκ τούτου, έχουν επιτύχει μία ομοιομορφία ως ένα βαθμό μεταξύ των διακρατικών νομοθετικών πρωτοβουλιών (UNCTAD, 2016). Ωστόσο, σημαντικό μειονέκτημα των κατευθυντήριων γραμμών του ΟΟΣΑ, αποτελεί ο μη δεσμευτικός χαρακτήρας αυτών, καθώς επαφίεται στη βούληση κάθε κράτους η υιοθέτηση τους και ο τρόπος ενσωμάτωσης των κανόνων και των αρχών τους (UNCTAD, 2016).

5.1.2 Η Σύμβαση 108 του Συμβουλίου της Ευρώπης

Το Συμβούλιο της Ευρώπης είναι ένας διεθνής οργανισμός, που ιδρύθηκε το 1949 με τη Συνθήκη του Λονδίνου και στο οποίο συμμετέχουν 46 κράτη της Ευρώπης και 5 κράτη ως παρατηρητές[47]. Το 1981 ψηφίστηκε η Σύμβαση για την Προστασία των Ατόμων σε σχέση με την Αυτόματη Επεξεργασία των Προσωπικών Δεδομένων, που συνήθως αναφέρεται ως Σύμβαση 108 του Συμβουλίου της Ευρώπης.

Η Σύμβαση 108[48], έχει υπογραφεί και επικυρωθεί από πενήντα πέντε κράτη[49], τα περισσότερα από τα οποία είναι ευρωπαϊκά, αλλά κάποια από αυτά είναι εκτός ευρωπαϊκών συνόρων. Η Σύμβαση 108 ορίζει ότι τα κράτη που έχουν υπογράψει τη Σύμβαση δεν μπορούν να περιορίσουν την ελεύθερη ροή προσωπικών δεδομένων μεταξύ τους[50]. Αντίθετα, η

[47] Στα μέλη του Συμβουλίου της Ευρώπης περιλαμβάνονται όλα τα ευρωπαϊκά κράτη εκτός της Λευκορωσίας, του Καζακστάν, της Πόλης του Βατικανού, της Ρωσίας, που αποβλήθηκε το 2022 λόγω της εισβολής στην Ουκρανία και των ευρωπαϊκών κρατών με περιορισμένη αναγνώριση, ενώ καθεστώς παρατηρητή έχει παραχωρηθεί στις Ηνωμένες Πολιτείες Αμερικής, την Αγία Έδρα, την Ιαπωνία, τον Καναδάς και το Μεξικό, https://www.coe.int/el/web/about-us/our-member-states (τελευταία προσπέλαση: 17 Απριλίου 2024)

[48] Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, Στρασβούργο, 21-1-1981, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108 (τελευταία προσπέλαση: 17 Απριλίου 2024)

[49] Η λίστα με τα κράτη που έχουν υπογράψει τη Σύμβαση 108 του Συμβουλίου της Ευρώπης είναι διαθέσιμη στο: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (τελευταία προσπέλαση: 17 Απριλίου 2024)

[50] Σύμβαση 108, άρθρο 12 παρ. 2

μεταφορά δεδομένων σε χώρες που δεν έχουν υπογράψει, επιτρέπεται μόνο εάν διασφαλίζεται επαρκές επίπεδο προστασίας των δεδομένων[51] (Kong, 2010).

Το 2018 επήλθε τροποποίηση στη Σύμβαση 108, που συνήθως αναφέρεται ως «Σύμβαση 108+»[52], και η οποία πρόκειται να τεθεί σε ισχύ με την κύρωση της από 38 κράτη[53]. Η νέα Σύμβαση 108+, εξακολουθεί να απαγορεύει τον αποκλεισμό της διασυνοριακής ροής μεταξύ των χωρών που έχουν υπογράψει τη Σύμβαση και να προβλέπει εξαίρεση σε περίπτωση που η μεταφορά δεδομένων θα μπορούσε να οδηγήσει σε καταστρατήγηση των διατάξεων της Σύμβασης. Μάλιστα, η τροποποιημένη σύμβαση προβλέπει ως πρόσθετη εξαίρεση από την απαγόρευση αποκλεισμού των διαβιβάσεων μεταξύ των μερών, την περίπτωση που ένα μέρος δεσμεύεται από εναρμονισμένους κανόνες προστασίας που μοιράζονται τα κράτη που ανήκουν σε περιφερειακό διεθνή οργανισμό[54].

Αυτό σημαίνει ότι όταν τεθεί σε ισχύ η Σύμβαση 108+ του 2018, οι υπογράφοντες τη Σύμβαση δεν δεσμεύεται να διασφαλίζουν την ελεύθερη ροή δεδομένων μεταξύ τους, εάν ισχύει μία από τις εξαιρέσεις. Η εξαίρεση που εισήχθη πρόσφατα, για παράδειγμα, ισχύει και για τα κράτη μέλη της Ευρώπης Ένωση (OECD, 2022).

Πλεονεκτήματα της Σύμβασης αποτελούν η δεσμευτική της φύση και το σαφές και πλήρες πλέγμα διατάξεών της. Αντιθέτως, βασικό μειονέκτημα θεωρείται η αδυναμία να αντιμετωπίσει τις δυσχέρειες που προκύπτουν από τα διαφορετικά νομοθετικά πλαίσια κάθε χώρας-μέλους (UNCTAD, 2016).

5.1.3 Η ρύθμιση των διασυνοριακών διαβιβάσεων από τον Γενικό Κανονισμό Προστασίας Δεδομένων

Η Ευρωπαϊκή Ένωση ρυθμίζει τη διασυνοριακή ροή δεδομένων μέσω του GDPR, ο οποίος περιέχει μια σειρά από μηχανισμούς που προβλέπονται στο Κεφάλαιο V (άρθρα 44 έως 49), οι οποίοι χρησιμοποιούνται από τρίτες χώρες και οργανισμούς τρίτων χωρών για την πραγματοποίηση διαβιβάσεων προσωπικών δεδομένων εκτός ΕΕ.

---

[51] Σύμβαση 108, άρθρο 12 παρ. 3

[52] Σύμβαση 108+ του Συμβουλίου της Ευρώπης, Σύμβαση για την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, Έλσινορ, 18-5-2018, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (τελευταία προσπέλαση: 17 Απριλίου 2024)

[53] Η Σύμβαση 108+ δεν έχει τεθεί ακόμη σε ισχύ, καθώς αναμένεται η κύρωσή της από 7 ακόμη κράτη, για να συμπληρωθούν τα 38 κράτη που αποτελούν προϋπόθεση για τη θέση σε ισχύ της Σύμβασης. Μέχρι σήμερα έχουν κυρώσει τη Σύμβαση 31 κράτη, μεταξύ των οποίων η Αλβανία, Ανδόρα, Αρμενία, Αυστρία, Βόρεια Μακεδονία, Βοσνία Ερζεγοβίνη, Βουλγαρία, Γαλλία, Γερμανία, Ελβετία, Εσθονία, Ισλανδία, Ισπανία, Ιταλία, Κροατία, Κύπρος, Λιθουανία, Λιχτενστάιν, Μάλτα, Ουγγαρία, Πολωνία, Πορτογαλία, Ρουμανία, Σαν Μαρίνο, Σερβία, Σλοβακία, Σλοβενία, Φινλανδία, καθώς και οι χώρες μη-μέλη του Συμβουλίου της Ευρώπης Αργεντινή, Μαυρίκιος και Ουρουγουάη, διαθέσιμο στο: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (τελευταία προσπέλαση: 17 Απριλίου 2024)

[54] Σύμβασης 108+, άρθρο 14

Η διασυνοριακές διαβιβάσεις δεδομένων κατ' αρχήν απαγορεύονται υπό το καθεστώς του GDPR, όπως προβλέπεται από το άρθρο 44, με την επιφύλαξη των εξαιρέσεων που αναφέρονται στα επόμενα άρθρα[55] (Juliussen, Kozyri, Johansen, Rui, 2023).

Αρχικά, σύμφωνα με το άρθρο 45 του Κανονισμού, η διαβίβαση δεδομένων προσωπικού χαρακτήρα επιτρέπεται σε χώρες που η Ευρωπαϊκή Επιτροπή έχει εκδώσει Απόφαση Επάρκειας, αφού εκτιμήσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας δεδομένων προσωπικού χαρακτήρα[56]. Σύμφωνα με την αιτιολογική σκέψη 104, η επάρκεια νοείται ως ουσιαστική ισοδυναμία μεταξύ του επιπέδου προστασίας προσωπικών δεδομένων και αυτού που διασφαλίζεται εντός της ένωσης[57]. Κατά την εκτίμηση της επάρκειας, η Επιτροπή λαμβάνει υπόψη μία σειρά παραγόντων, συμπεριλαμβανομένων, των νομοθεσιών όσον αφορά τη δημόσια ασφάλειας, το ποινικό δίκαιο, τους κανόνες περί προστασίας δεδομένων, την ύπαρξη ανεξάρτητων εποπτικών αρχών και τις διεθνείς δεσμεύσεις που έχει αναλάβει η τρίτη χώρα[58]. Η Ευρωπαϊκή Επιτροπή θεωρεί ότι μία Απόφαση Επάρκειας είναι η καλύτερη οδός για την οικοδόμηση αμοιβαίας εμπιστοσύνης, τη διασφάλιση της απρόσκοπτης ροής προσωπικών δεδομένων και, συνεπώς, τη διευκόλυνση των εμπορικών ανταλλαγών που περιλαμβάνουν διαβιβάσεις προσωπικών δεδομένων[59] (Sullivan, 2019).

Ελλείψει απόφασης επάρκειας, η διασυνοριακή ροή επιτρέπεται, βάσει του GDPR, εφόσον ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει παράσχει κατάλληλες εγγυήσεις[60]. Οι κατάλληλες εγγυήσεις παρέχονται μέσω:

- νομικά δεσμευτικού και εκτελεστού μέσου μεταξύ δημόσιων αρχών,
- δεσμευτικών εταιρικών κανόνων (Binding Corporate Rules - BCR),
- τυποποιημένων συμβατικών ρητρών προστασίας δεδομένων (Standard Contract Clauses - SCCs),
- εγκεκριμένου κώδικα δεοντολογίας,

[55] GDPR, άρθρο 44

[56] GDPR, άρθρο 45 παρ. 1

[57] Αιτιολογική σκέψη 104 του GDPR, «Η έκδοση απόφασης επάρκειας για ένα έδαφος ή συγκεκριμένο τομέα τρίτης χώρας θα πρέπει να συνεκτιμά σαφή και αντικειμενικά κριτήρια, όπως συγκεκριμένες δραστηριότητες επεξεργασίας και το πεδίο εφαρμογής των εφαρμοστέων νομικών προτύπων και της νομοθεσίας που ισχύουν στην τρίτη χώρα. Η τρίτη χώρα θα πρέπει να προσφέρει εγγυήσεις που να διασφαλίζουν ένα κατάλληλο επίπεδο προστασίας, ουσιωδώς ισοδύναμο με αυτό που διασφαλίζεται εντός της Ένωσης, ιδίως όταν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα γίνεται σε έναν ή διαφόρους συγκεκριμένους τομείς. Ειδικότερα, η τρίτη χώρα θα πρέπει να διασφαλίζει την αποτελεσματική ανεξάρτητη εποπτεία της προστασίας των δεδομένων και να προβλέπει μηχανισμούς συνεργασίας με τις αρχές προστασίας δεδομένων των κρατών μελών, τα δε υποκείμενα των δεδομένων θα πρέπει να έχουν στη διάθεσή τους αποτελεσματικά και νομικώς ισχυρά δικαιώματα, καθώς και τη δυνατότητα άσκησης αποτελεσματικών διοικητικών και δικαστικών προσφυγών.»

[58] GDPR, άρθρο 45 παρ. 2

[59] Ευρωπαϊκή Επιτροπή, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, «Ανταλλαγή και προστασία των δεδομένων προσωπικού χαρακτήρα σε έναν παγκοσμιοποιημένο κόσμο», 10.1.2017 COM (2017) 7 final, https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A52017DC0007 (τελευταία προσπέλαση: 9 Ιουνίου 2024)

[60] GDPR, άρθρο 46

- εγκεκριμένου μηχανισμού πιστοποίησης.

Αναφορικά με τους δεσμευτικούς εταιρικούς κανόνες, ο GDPR καθορίζει το ελάχιστο περιεχόμενο τους, στους οποίους πρέπει να αναφέρονται η δομή και τα στοιχεία επικοινωνίας για τις ενδιαφερόμενες εταιρείες, η εφαρμογή των γενικών αρχών προστασίας προσωπικών δεδομένων, τα δικαιώματα των υποκειμένων, διαδικασίες καταγγελίας και μηχανισμοί συμμόρφωσης[61]. Ως εκ τούτου, οι BCR έχουν ομοιότητες με το σύστημα CBPR της APEC, που θα αναλυθεί κατωτέρω (Sullivan, 2019). Οι οργανισμοί που υιοθετούν BCR πρέπει να αποδείξουν ότι είναι δεσμευτικές και επιβάλλονται και στις θυγατρικές εταιρείες του και στους εργαζομένους τους και ότι θεσπίζουν δικαιώματα για τα υποκείμενα των δεδομένων[62].

Σύμφωνα με τα άρθρα 40 και 41 του GDPR, επιτρέπεται η χρήση κώδικα δεοντολογίας, που μπορεί να εκπονηθεί από ενώσεις και άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία, εφαρμόζοντας τις απαιτήσεις του Κανονισμού. Στην περίπτωση αυτή, το προσχέδιο του κώδικα πρέπει να υποβληθεί στην αρμόδια εποπτική αρχή για να προσδιοριστεί εάν παρέχει επαρκείς και κατάλληλες ασφαλιστικές δικλείδες[63]. Οι εγκεκριμένοι κώδικες δεοντολογίας πρέπει να επιτρέπουν την παρακολούθηση της συμμόρφωσης των υπεύθυνων επεξεργασίας με τις διατάξεις του από το φορέα παρακολούθησης, που πρέπει να είναι διαπιστευμένος από την αρμόδια εποπτική αρχή, αφού αποδείξει το κατάλληλο επίπεδο εμπειρογνωμοσύνης σε σχέση με το αντικείμενο του κώδικα[64].

Ένας άλλος μηχανισμός που έχει ιδιαίτερη σημασία για τις εταιρείες που επεξεργάζονται και μεταφέρουν προσωπικά δεδομένα, είναι η πιστοποίηση που προβλέπεται στο άρθρο 42 του GDPR. Η πιστοποίηση είναι εθελοντική και χορηγείται από τους φορείς πιστοποίησης ή την αρμόδια εποπτική αρχή ή Συμβούλιο Προστασίας Δεδομένων για μέγιστη περίοδο τριών ετών, ενώ μπορεί να ανανεωθεί, εφόσον εξακολουθούν να πληρούνται οι σχετικές απαιτήσεις[65].

5.1.4 Το Πλαίσιο Προστασίας Προσωπικών Δεδομένων της APEC (CBPR)

Ένα άλλο πλαίσιο ρύθμισης της διασυνοριακής ροής είναι το Σύστημα Διασυνοριακών Κανόνων Απορρήτου (CBPR) της Οικονομικής Συνεργασίας Ασίας - Ειρηνικού (APEC). Η Οικονομική Συνεργασία Ασίας - Ειρηνικού (APEC) είναι ένα διακυβερνητικό οικονομικό φόρουμ που ιδρύθηκε το 1989 σε απάντηση της αυξανόμενης αλληλεξάρτησης των οικονομιών της Ασίας και του Ειρηνικού. Ως όργανο, η APEC δεν έχει την αυστηρή διαστρωμάτωση της Ευρωπαϊκής Ένωσης, ούτε έχει νομοθετικές εξουσίες και εκτελεστικούς μηχανισμούς. Η APEC έχει επί του παρόντος 21 μέλη[66], στα οποία περιλαμβάνονται η Κίνα, η Ιαπωνία, η Κορέα, η Ταϊλάνδη, οι Ηνωμένες Πολιτείες Αμερικής, ο Καναδάς, το Μεξικό και η Ρωσία. Ο κυρίαρχος στόχος της APEC είναι η ανάπτυξη της οικονομίας των χωρών της Ασίας και του Ειρηνικού. Στο πλαίσιο αυτό, ιδρύθηκε το 2012 το Σύστημα Διασυνοριακών

[61] GDPR, άρθρο 47 παρ. 2
[62] GDPR, άρθρο 47 παρ. 1
[63] GDPR, άρθρο 40
[64] GDPR, άρθρο 41
[65] GDPR, άρθρο 42
[66] APEC «Μέλη-Οικονομίες», https://www.apec.org/about-us/about-apec/member-economies (τελευταία προσπέλαση: 17 Απριλίου 2024)

Κανόνων Απορρήτου (CBPR) της APEC για τη διευκόλυνση των διασυνοριακών ροών δεδομένων μεταξύ των μελών-οικονομιών που πληρούν τα πρότυπα προστασίας δεδομένων που προβλέπονται από το σύστημα αυτό (Sullivan, 2019).

Το CBPR βασίζεται στις αρχές προστασίας δεδομένων που ορίζονται στο Πλαίσιο Προστασίας Προσωπικών Δεδομένων της APEC (Πλαίσιο), ένα σύνολο αρχών και κατευθυντήριων γραμμών εφαρμογής που δημιουργήθηκε το 2005 και τροποποιήθηκε δέκα χρόνια αργότερα. Σε αντίθεση με τον GDPR, το Πλαίσιο της APEC δεν εφαρμόζεται ως νόμος, αλλά αποτελεί ένα συμφωνημένο πρότυπο, που ορίζει τα βασικά πρότυπα για την ελάχιστη προστασία δεδομένων, τα οποία οι οικονομίες-μέλη της APEC συμφωνούν να χρησιμοποιούν για τη διαμόρφωση του εσωτερικού δικαίου τους. Εφόσον δεν υπάρχει εσωτερική νομοθεσία ή όπου το εφαρμοστέο δίκαιο προβλέπει περιορισμένη προστασία για τα υποκείμενα των δεδομένων, το Πλαίσιο παρέχει ένα ελάχιστο επίπεδο προστασίας δεδομένων (Sullivan, 2019).

Το σύστημα CBPR αποτελείται από τρία στοιχεία: πρώτον, το Πλαίσιο που καθορίζει τις βασικές απαιτήσεις προστασίας δεδομένων, δεύτερον ένα σύστημα επιλογής και διαπίστευσης των υπεύθυνων λογοδοσίας, που είναι τρίτα ανεξάρτητα και αναγνωρισμένοι από την APEC μέρη, που διαθέτουν τα κατάλληλα προσόντα να αξιολογούν και να πιστοποιούν εταιρικές πρακτικές απορρήτου σύμφωνα με το Πλαισίου και το τρίτο στοιχείο είναι ένας εθνικός μηχανισμός επιβολής[67]. Προκειμένου μια οικονομία-μέλος της APEC να ενταχθεί στο σύστημα, υπάρχουν συγκεκριμένες απαιτήσεις, συμπεριλαμβανομένης της ύπαρξης μιας εθνικής αρχής επιβολής του νόμου και εθνικής νομοθεσίας, στην οποία εμπεριέχεται η ελάχιστη προστασία δεδομένων που προβλέπεται από το Πλαίσιο της APEC. Επιπλέον, η οικονομία της APEC πρέπει επίσης να υποδείξει έναν υπεύθυνο λογοδοσίας που πιστοποιεί τις πρακτικές απορρήτου των εταιρειών, που θέλουν να ενταχθούν στο σύστημα CBPR (Sullivan, 2019).

Μια εταιρεία που επιθυμεί να ενταχθεί στο CBPR οφείλει να θεσπίσει την πολιτική απορρήτου και να διαμορφώσει τις πρακτικές της ώστε να συμμορφώνεται είτε με τους βασικούς κανόνες του Πλαισίου ή την εθνική νομοθεσία, όποιο από τα δύο συνεπάγεται περισσότερη προστασία της ιδιωτικής ζωής. Στη συνέχεια η εταιρική πολιτική αξιολογείται από τους υπεύθυνους λογοδοσίας για να πιστοποιηθεί στο πλαίσιο του CBPR. Η διαδικασία αξιολόγησης και συμμόρφωσης με το CBPR είναι ολοκληρωμένη και χρονοβόρα τόσο για την εταιρεία όσο και για τον υπεύθυνο λογοδοσίας. Το κόστος εξαρτάται από τον οργανισμό, την επιχείρηση, τις δραστηριότητές και τους εσωτερικούς της πόρους, αλλά μπορεί να είναι μια δαπανηρή διαδικασία. Τουλάχιστον βραχυπρόθεσμα, αυτό γενικά περιορίζει τον CBPR σε οργανισμούς που έχουν τα απαραίτητα κεφάλαια και πόρους. Στις ΗΠΑ, για παράδειγμα, οι εταιρείες που έχουν ενταχθεί στο σύστημα CBPR είναι συνήθως μεγάλες πολυεθνικές εταιρείες, κυρίως τεχνολογικές (Sullivan, 2019).

Ενώ υπάρχουν παρόμοια εθελοντικά συστήματα στο πλαίσιο του GDPR, το CBPR είναι γενικά πιο ελκυστικό για τις αμερικανικές εταιρείες, ιδίως για τις μεγάλες πολυεθνικές που μπορούν να αντέξουν οικονομικά τη διαδικασία διαπίστευσης, καθώς θεωρείται λιγότερο πολύπλοκο και διευκολύνει περισσότερο τις διασυνοριακές ροές δεδομένων σε

[67] Πλαίσιο της APEC, μέρος 2ο, τμήμα 12ο

σύγκριση με το μοντέλο της ΕΕ. Σε αντίθεση με τον GDPR, που στοχεύσει στην προστασία των προσωπικών δικαιωμάτων ως ατομικό δικαίωμα των υποκειμένων, το CBPR έχει σχεδιαστεί κυρίως για να διευκολύνει τη διασυνοριακή ροή δεδομένων και θεσπίστηκε ρητά για να διαμορφώσει μία ισορροπία μεταξύ της προστασίας της ιδιωτικής ζωής και της αποφυγής των εμποδίων για την ροή πληροφοριών, προκειμένου να διασφαλιστεί η συνέχιση του εμπορίου και της οικονομικής ανάπτυξης στην περιοχή του APEC (Sullivan, 2019).

Ωστόσο, αν και οι γενικοί στόχοι προστασίας των δεδομένων του CBRP της APEC και των μηχανισμών του GDPR είναι αντίστοιχοι, η εφαρμογή των καθεστώτων διαφέρουν σημαντικά. Το CBPR βασίζεται στις αρχές προστασίας δεδομένων του Πλαισίου της APEC, το οποίο αποτελεί ένα βασικό πρότυπο προστασίας δεδομένων, το οποίο δεν είναι τόσο περιεκτικό, ούτε έχει άμεση δεσμευτική ισχύ όπως ο GDPR. Επιπλέον, το νομικό θεμέλιο της προσέγγισης της ΕΕ είναι θεμελιωδώς διαφορετικό από εκείνο του συστήματος της APEC. Ο Κανονισμός της ΕΕ βασίζεται στο θεμελιώδες δικαίωμα της προστασίας των δεδομένων και το δικαίωμα στην ιδιωτική ζωή. Από την άλλη πλευρά, η εστίαση της APEC τείνει περισσότερο προς τη διευκόλυνση της διαβίβασης δεδομένων εντός των παραμέτρων που θεωρεί αποδεκτές για την προστασία των δεδομένων[68] (Sullivan, 2019).

Συνοψίζοντας, το CBPR έχει ιδιάζουσα σημασία για τη ρύθμιση των διασυνοριακών ροών, δεδομένου ότι είναι μία από τις λίγες πρωτοβουλίες προστασίας δεδομένων που έχει τη στήριξη των ΗΠΑ, για το λόγο ότι παρέχει τεράστια ευελιξία κατά την εφαρμογή του. Παρόλα αυτά, σημαντικό μειονέκτημα του CBPR είναι ο μη δεσμευτικός χαρακτήρας του (UNCTAD, 2016).

5.1.5 Το Πλαίσιο Προστασίας Προσωπικών Δεδομένων της ASEAN

Η Ένωση των Χωρών της Νοτιοανατολικής Ασίας (Association of Southeast Asian Nations, ASEAN) είναι ένας διεθνής οικονομικός οργανισμός χωρών της Νοτιοανατολικής Ασίας, που δημιουργήθηκε το 1967, με πρωτοβουλία της Ινδονησίας, της Σιγκαπούρης, της Μαλαισίας, της Ταϊλάνδης και των Φιλιππίνων και αποτελείται από 10 μέλη-χώρες[69].

Το Πλαίσιο της ASEAN για την Προστασία Προσωπικών Δεδομένων επιδιώκει την ενίσχυση της προστασίας των δεδομένων προσωπικού χαρακτήρα στις χώρες της ASEAN και τη διευκόλυνση της συνεργασίας μεταξύ των συμμετεχόντων χωρών. Το Πλαίσιο δεν δημιουργεί νομικά δεσμευτικές υποχρεώσεις, αλλά ενθαρρύνει τη συνεργασία των οικονομιών που συμμετέχουν και την προώθηση και εφαρμογή των αρχών απορρήτου που ορίζονται στο Πλαίσιο, ενώ διασφαλίζει την ελεύθερη ροή πληροφοριών μεταξύ των κρατών μελών της ASEAN (ASEAN, 2018).

[68] Αυτό είναι εμφανές σε έναν από τους διακηρυγμένους στόχους του CBPR της APEC, που είναι η προώθηση «ενός προτύπου πολιτικής που αποσκοπεί στη διασφάλιση της συνεχούς ελεύθερης διασυνοριακής ροής των προσωπικών πληροφοριών, με ταυτόχρονη καθιέρωση ουσιαστικής προστασίας της ιδιωτικής ζωής και της ασφάλειας των προσωπικών δεδομένων», APEC Privacy Framework 2015

[69] Μέλη της ASEAN αποτελούν: το Βιετνάμ, η Ινδονησία, η Καμπότζη, η Λαϊκή Δημοκρατία του Λάος, η Μαλαισία, το Μπρουνέι, η Μιανμάρ, η Σιγκαπούρη, η Ταϊλάνδη και οι Φιλιππίνες, https://asean.org/about-us/ (τελευταία προσπέλαση: 17 Απριλίου 2024)

Τον Ιανουάριο του 2021, η πρώτη Σύνοδος Υπουργών Ψηφιακών Υπουργών της ASEAN, ενέκρινε επίσης την Πλαίσιο Διαχείρισης Δεδομένων (Digital Management Framework - DMF) (ASEAN, 2021) και Υπόδειγμα Συμβατικών Ρητρών για Διασυνοριακές Ροές Δεδομένων (ASEAN, 2021). Ειδικότερα, το Υπόδειγμα της ASEAN είναι υπόδειγμα συμβατικών όρων και προϋποθέσεων που ενδέχεται να περιλαμβάνονται στις νομικά δεσμευτικές συμφωνίες μεταξύ επιχειρήσεων που διαβιβάζουν προσωπικά δεδομένα η μία στην άλλη διασυνοριακά και αποτελεί το βασικό εργαλείο για τις διασυνοριακές ροές δεδομένων από τις επιχειρήσεις της ASEAN. Αυτό συμβάλλει στη μείωση του κόστους και του χρόνου διαπραγμάτευσης και συμμόρφωσης, ενώ διασφαλίζει την προστασία των προσωπικών δεδομένων κατά τη διασυνοριακή μεταφορά δεδομένων (OECD, 2022).

5.2 Η διαβίβαση προσωπικών δεδομένων μεταξύ Ευρωπαϊκής Ένωσης και Ηνωμένων Πολιτειών Αμερικής

5.2.1 Το Safe Harbour και η ακύρωσή του από την απόφαση Schrems I

Οι διαβιβάσεις των δεδομένων προσωπικού χαρακτήρα μεταξύ των ΗΠΑ και της ΕΕ παρουσιάζουν ιδιαίτερο ενδιαφέρον, δεδομένου του τεράστιου μεγέθους των δύο οικονομιών σε συνάρτηση με την εμφανώς διαφορετική προσέγγιση που έχουν υιοθετήσει οι δύο οικονομίες αναφορικά με την προστασία προσωπικών δεδομένων. Μετά την υιοθέτηση της Οδηγίας 95/46/ΕΚ στην Ευρωπαϊκή Ένωση, η οποία εισήγαγε αυστηρές ρυθμίσεις αναφορικά με την προστασία δεδομένων, ανέκυψε το ζήτημα σχετικά με τη νομιμότητα των διαβιβάσεων προσωπικών δεδομένων των ευρωπαίων πολιτών στις ΗΠΑ για τη δραστηριοποίηση των αμερικάνικων εταιρειών στην Ευρωπαϊκή Ένωση, που η αγορά της αποτελεί πόλο έλξης για τις εταιρείες διεθνώς.

Σύμφωνα με τη νομοθεσία της ΕΕ και πιο συγκεκριμένα το άρθρο 26 της Οδηγίας 95/46/ΕΚ σε γενικές γραμμές τρεις μηχανισμοί που επιτρέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από την ΕΕ σε τρίτο κράτος. Πρώτον, οι διαβιβάσεις σε κράτος εκτός ΕΕ μπορούν να βασίζονται σε γνώμη της Επιτροπής με την οποία διαπιστώνεται ότι το τρίτο κράτος διασφαλίζει επαρκές επίπεδο προστασίας. Ελλείψει τέτοιας απόφασης, η διαβίβαση μπορεί να πραγματοποιηθεί όταν συνοδεύεται από κατάλληλες διασφαλίσεις, για παράδειγμα τυποποιημένες συμβατικές ρήτρες (Standard Contract Clauses - SCCs), και ελλείψει τέτοιων εγγυήσεων, βάσει ορισμένων παρεκκλίσεων για συγκεκριμένες περιπτώσεις[70] (Tzanou, 2020).

Δεδομένου ότι η εσωτερική νομοθεσία των ΗΠΑ δεν ήταν δυνατό να εγγυηθεί ίσο επίπεδο προστασίας με αυτό της Ευρωπαϊκής Ένωσης, δεν υπήρχε επίσημη διαπίστωση επάρκειας όσον αφορά την προστασία της ιδιωτικής ζωής των δεδομένων στις ΗΠΑ. Στο πλαίσιο αυτό, την 21η Ιουλίου 2000 υιοθετήθηκε η Συμφωνία «Ασφαλούς Λιμένα»[71] (Safe

[70] Οδηγίας 95/46/ΕΚ, άρθρο 26

[71] Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000 (2000/520/ΕΚ), 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 εδώ https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32000D0520 (τελευταία προσπέλαση: 21 Απριλίου 2024)

Harbor Agreement) μεταξύ της ΕΕ και των ΗΠΑ, προκειμένου να καθίσταται εφικτή η διασυνοριακή δεδομένων των πολιτών της ΕΕ στις ΗΠΑ και να επιτραπεί το διεθνές εμπόριο.

Το Safe Harbour βασίστηκε σε ένα σύστημα εθελοντικής αυτοπιστοποίησης και αυτοαξιολόγησης των εταιρειών που εδρεύουν στις ΗΠΑ ότι τηρούν ορισμένα μέτρα προστασίας δεδομένων, τις «αρχές του ασφαλούς λιμένα», σε συνδυασμό με κάποια παρέμβαση των δημοσίων αρχών. Ειδικότερα, στο πλαίσιο του συστήματος αυτού, οι αμερικανικές εταιρείες έπρεπε να καταγράφουν τη συμμόρφωσή τους με τις αρχές του ασφαλούς λιμένα στο Υπουργείο των ΗΠΑ, ενώ η FTC ήταν υπεύθυνη για την επιβολή της συμφωνίας. Με βάση το σύστημα αυτό, η Επιτροπή εξέδωσε την απόφαση Safe Harbour, αναγνωρίζοντας την επάρκεια της προστασίας που παρέχουν οι αρχές του Ασφαλούς Λιμένα. Το Safe Harbour αποδείχθηκε σημαντικό εργαλείο των διατλαντικών εμπορικών σχέσεων, με περισσότερες από 3200 εταιρείες να υπογράφουν το σύστημα (Tzanou, 2020).

Ωστόσο, διαπιστώθηκε ότι υφίσταντο σημαντικές αδυναμίες όσον αφορά τη συμμόρφωση των αυτοπιστοποιούμενων εταιρειών και την επιβολή και εποπτεία από τις αρμόδιες αρχές των ΗΠΑ. Ειδικότερα, η απόφαση 2000/520, δεν περιλάμβανε δύο σημαντικές πτυχές. Πρώτον, δεν διαπιστώνει την ύπαρξη κανόνων στις Ηνωμένες Πολιτείες που στοχεύουν στον περιορισμό οποιασδήποτε παραβίασης των θεμελιωδών δικαιωμάτων ατόμων των οποίων τα δεδομένα μεταφέρονται από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες. Δεύτερον, δεν αναφέρει την ύπαρξη ενός ισχυρού δικαστικού συστήματος που μπορεί να παρέχει επαρκή προστασία έναντι τέτοιων παρεμβάσεων. Ως εκ τούτου, παραβιάζονται ευθέως τα άρθρα 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων, τα οποία υπογραμμίζουν την ανάγκη για σαφείς και συγκεκριμένους κανόνες που διέπουν το πεδίο εφαρμογής και την εφαρμογή των σχετικών μέτρων, ενώ επιβάλλουν την εξασφάλιση επαρκών διασφαλίσεων για τα άτομα των οποίων τα δεδομένα διατηρούνται. Αυτές οι διασφαλίσεις αποσκοπούν στην αποτελεσματική προστασία από τους κινδύνους κακής χρήσης, μη εξουσιοδοτημένης πρόσβασης και μη εξουσιοδοτημένης χρήσης προσωπικών δεδομένων (Τάσσης, 2015).

Οι ελλείψεις αυτές της Συμφωνίας «Ασφαλούς Λιμένα», δημιούργησαν πρόσθετες ανησυχίες σχετικά με τη συστηματική πρόσβαση των αρχών επιβολής του νόμου των ΗΠΑ σε δεδομένα που κατέχουν οι ιδιωτικές εταιρείες που έχουν πιστοποιηθεί στο πλαίσιο του συστήματος[72] (Τάσσης, 2015). Ως εκ τούτου, το Δικαστήριο της Ευρωπαϊκής Ένωσης στην υπόθεση Schrems I, κλήθηκε να αποφανθεί σχετικά με τη συμβατότητα της Συμφωνίας αυτής με την ευρωπαϊκή νομοθεσία και αφού διαπίστωσε πως οι διαβιβάσεις των δεδομένων στις ΗΠΑ βάσεις της Safe Harbor, ελλόχευε σημαντικούς κινδύνους για την προστασία της ιδιωτικής ζωής των πολιτών της ΕΕ, ακύρωσε τη συμφωνία αυτή με την απόφαση του στην υπόθεση C- 362/14 γνωστή ως «Schrems I»[73].

[72] Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο όσον αφορά τη λειτουργία του ασφαλούς λιμένα από τη σκοπιά των πολιτών της Ένωσης και των εταιρειών που είναι εγκατεστημένες στην ΕΕ/COM/2013/847 final/, διαθέσιμο εδώ https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52013DC0847 (τελευταία προσπέλαση: 21 Απριλίου 2024)

[73] Απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης της 6ης Οκτωβρίου 2015 στην υπόθεση C-362/14, στο πλαίσιο της δίκης Maximillian Schrems κατά Data Protection Commissioner, διαθέσιμο στο:

Η υπόθεση Schrems I προέκυψε μετά τις αποκαλύψεις του Edward Snowden το 2013, ότι η National Security Agency (NSA) είχε εφαρμόσει μυστικά προγράμματα παρακολούθησης που της επέτρεπαν τη μαζική παρακολούθηση πολιτών της ΕΕ μέσω άμεσης πρόσβασης στους κεντρικούς διακομιστές κορυφαίων αμερικανικών τεχνολογικών κολοσσών, όπως το Facebook, το Skype, η Microsoft και η Yahoo[74] (Kuner, 2017). Ο Max Schrems, ένας αυστριακός φοιτητής νομικής τότε, που ήταν συνδρομητής στο κοινωνικό δίκτυο Facebook από το 2008, ασχολήθηκε ιδιαίτερα με τη συμμόρφωση της εταιρείας που είχε έδρα στην Αμερική, με την ευρωπαϊκή νομοθεσία. Αξιοποιώντας το δικαίωμα πρόσβασης που του διασφαλίζοντας από την Οδηγία 95/46/ΕΚ, ζήτησε από την εταιρεία να του παραδώσει τα προσωπικά τα δεδομένα που κατείχε, και έλαβε 1.200 σελίδες με προσωπικές πληροφορίες (Calia, 2021). Κατόπιν τούτου και μετά τις αποκαλύψεις του Snowden, κατέθεσε καταγγελία στον Ιρλανδό Επίτροπο Προστασίας Δεδομένων (Data Protection Commission - DPC) τον Ιούνιο του 2013, ζητώντας του να απαγορεύσει στο Facebook Ireland να διαβιβάσει τα προσωπικά του δεδομένα στις ΗΠΑ, όπου θα μπορούσαν να αποτελέσουν αντικείμενο παρακολούθησης από την NSA. Ο Επίτροπος απέρριψε την καταγγελία του Schrems με το σκεπτικό ότι δεν ήταν νόμω βάσιμη. Ο Schrems προσέφυγε κατά της απόφασης της DPC στο Ανώτατο Δικαστήριο της Ιρλανδίας, το οποίο αποφάσισε να αναστείλει τη διαδικασία και να παραπέμψει το ζήτημα στο ΔΕΕ μετά την διαδικασία προδικαστικής παραπομπής (Tzanou, 2020).

Το ΔΕΕ εξέδωσε την απόφασή του το 2015, καταλήγοντας στο συμπέρασμα ότι οι αμερικανικές αρχές είχαν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που διαβιβάστηκαν από τα κράτη μέλη της ΕΕ και υπήρχε η δυνατότητα να τα επεξεργάζονται πέραν του απολύτως αναγκαίου και αναλογικού σε σχέση με την προστασία της εθνικής ασφάλειας (Tzanou, 2020).

Όπως αναφέρθηκε ανωτέρω, η απόφαση της Επιτροπής Safe Harbour τελικά ακυρώθηκε από το ΔΕΕ με την απόφαση Schrems I που εκδόθηκε στις 6 Οκτωβρίου 2015. Στην εν λόγω υπόθεση, το Δικαστήριο βρήκε την ευκαιρία να διευκρινίσει το κριτήριο της επάρκειας. Αν και σημείωσε ότι δεν προβλεπόταν από το νόμο ορισμός της έννοιας του επαρκούς επιπέδου προστασίας[75], το ΔΕΕ παρατήρησε ότι η επάρκεια δεν απαιτεί ένα επίπεδο προστασίας πανομοιότυπο με εκείνο που εγγυάται η έννομη τάξη της ΕΕ, αλλά ένα επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών που είναι «ουσιαστικά ισοδύναμο» με εκείνο της ΕΕ[76]. Ως εκ τούτου, απαιτείται αξιολόγηση του περιεχομένου της εφαρμοστέας εθνικής νομοθεσίας στην τρίτη χώρα, καθώς και της πρακτικής που αποσκοπεί στη διασφάλιση συμμόρφωσης με τους εν λόγω κανόνες. Το κριτήριο της «ουσιαστικής ισοδυναμίας» δείχνει ότι το Δικαστήριο προσπαθεί να φέρει τα εξωτερικά νομικά συστήματα όσο το δυνατόν πιο κοντά στα εσωτερικά δεδομένα της ΕΕ, σχετικά με το νομικό πλαίσιο για την προστασία των δεδομένων, προκειμένου να διασφαλιστεί ότι οι

https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62014CJ0362 (τελευταία προσπέλαση: 21 Απριλίου 2024)

[74] Glenn Greenwald and Ewen MacAskill, «NSA Prism program taps in to user data of Apple, Google and others», The Guardian, 7 June 2013, διαθέσιμο εδώ https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, (τελευταία προσπέλαση: 21 Απριλίου 2024)

[75] C-362/14 (Schrems I), para 70

[76] ό.π., para 73

εγχώριοι κανόνες προστασίας δεδομένων δεν καταστρατηγούνται από τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από την ΕΕ σε τρίτες χώρες[77].

Η εξωεδαφική προσέγγιση αυτή, που έχει ακολουθηθεί και σε άλλες αποφάσεις του ΔΕΕ, όπως στην υπόθεση Google Spain[78] συνδέεται στενά με την αναβάθμιση της προστασίας των δεδομένων σε επίπεδο θεμελιώδους δικαιώματος που καθιστά την άσκηση της δικαιοδοσίας της ΕΕ, όχι απλώς επιτρεπτή, (διακριτική ευχέρεια), αλλά και υποχρεωτική (Ryngaert, Taylor, 2019). Αυτό σημαίνει αναγκαστικά ότι η διασυνοριακή ροή δεδομένων θα πρέπει να θεωρείται ως μέρος των θεμελιωδών δικαιωμάτων προστασίας των θεσμικών οργάνων της ΕΕ (Kuner, 2013). Πράγματι, το Δικαστήριο δήλωσε ότι τα άτομα δεν μπορούν να στερηθούν τα θεμελιώδη δικαιώματά τους από τη διαβίβαση των δεδομένων τους σε τρίτες χώρες[79].

Στην υπόθεση Schrems I, το Δικαστήριο αμφισβήτησε τη συμβατότητα της απόφασης Ασφαλούς Λιμένα με την ευρωπαϊκή νομοθεσία και ειδικότερα με την Οδηγία 95/46/ΕΚ, χωρίς να αποφαίνεται σχετικά με το κατά πόσο εξασφαλίζεται επαρκώς η προστασία δεδομένων από τη νομοθεσία των ΗΠΑ (Tzanou, 2020). Το ΔΕΕ κατά την αξιολόγηση της συμφωνίας Ασφαλούς Λιμένα, τόνισε τρεις σημαντικές ελλείψεις (αναγνωρίζοντας ότι σχετίζονται επίσης με ελλείψεις στον έλεγχο της Επιτροπής): πρώτον, έλλειψη ρητών νομοθετικών διατάξεων στην εσωτερική νομοθεσία των ΗΠΑ σχετικά με την απαίτηση να διασφαλίζεται επαρκής προστασία των προσωπικών δεδομένων, δεύτερον, διαπίστωσε ότι οι όροι για την παράκαμψη των υποχρεώσεων της συμφωνίας στο όνομα της εθνικής ασφάλειας ήταν υπερβολικά επιεικείς, και τρίτον την απουσία διαδικασίας που να επιτρέπει προσφυγές από πολίτες της ΕΕ (Τάσσης, 2015).

Αδιαμφησβήτητα, η απόφαση Schrems I αποτελεί θεμελιώδη λίθο για την προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ από τις διαβιβάσεις σε τρίτες χώρες (Kuner, 2017). Με την απόφαση αυτή, αναγνωρίστηκε η εξωεδαφική εφαρμογή των θεμελιωδών δικαιωμάτων της ΕΕ και κατέστη σαφές ότι η διαβίβαση των προσωπικών δεδομένων είναι νόμιμη μόνο ο εφόσον διασφαλίζεται η επαρκής προστασία των θεμελιωδών δικαιωμάτων της ΕΕ. Ωστόσο, η κρίση του ΔΕΕ στην υπόθεση Schrems I, έχει επικριθεί από πολλούς θεωρητικούς, καθώς το ΔΕΕ επέλεξε να βασίσει την απόφασή του σε μία γενική ρήση ότι με τις διαβιβάσεις προσωπικών δεδομένων στις ΗΠΑ παραβιάζεται η «ουσία» του θεμελιώδους δικαιώματος της ιδιωτικής ζωής και της αποτελεσματικής δικαστικής προστασίας σύμφωνα με το ΧΘΔ, χωρίς να εξειδικεύσει επαρκώς το περιεχόμενο της ιδιωτικής ζωής και χωρίς να εξετάσει ενδελεχώς το νομοθετικό πλαίσιο των ΗΠΑ και κατά πόσο αυτό θεωρείται επαρκές για την προστασία των προσωπικών δεδομένων (Tzanou, 2020).

5.2.2 Η EU-U.S. Privacy Shield και η ακύρωσή της με την απόφαση Schrems II

Μετά από δύο χρόνια διαπραγματεύσεων, η Ευρωπαϊκή Επιτροπή και το Υπουργείο Εμπορίου των ΗΠΑ στις 2 Φεβρουαρίου 2016 πέτυχαν μια συμφωνία για ένα νέο πλαίσιο για

[77] ό.π.

[78] Απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης της 13ης Μαΐου στην υπόθεση C-131/12, στο πλαίσιο της δίκης Google Spain SL κατά Agencia Española de Protección de Datos (AEPD), https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62012CJ0131, (τελευταία προσπέλαση: 21 Απριλίου 2024)

[79] C-362/14 (Schrems I), para 58

τις διατλαντικές ανταλλαγές προσωπικών δεδομένων για εμπορικούς σκοπούς: την Ασπίδα Προστασίας της Ιδιωτικής Ζωής (Privacy Shield) ΕΕ-ΗΠΑ (IP/16/216)[80]. Αυτό το πλαίσιο είχε ως σκοπό την προστασία των θεμελιωδών δικαιωμάτων των ατόμων όπου τα δεδομένα τους μεταφέρονται στις Ηνωμένες Πολιτείες και την εξασφάλιση ενός κατανοητού και ασφαλούς νομικού πλαισίου για τις επιχειρήσεις. Στις 12 Ιουλίου 2016, μετά από θετική ψήφο από τα Κράτη Μέλη, το Σώμα των Επιτρόπων επίσημα ενέκρινε την Ασπίδα Προστασίας της Ιδιωτικής Ζωής ΕΕ-ΗΠΑ.

Η Ασπίδα Προστασίας της Ιδιωτικής Ζωής ΕΕ-ΗΠΑ τέθηκε σε εφαρμογή για να αντικαταστήσει τις Διεθνείς Αρχές Προστασίας της Ιδιωτικής Ζωής Ασφαλούς Λιμένα, οι οποίες κηρύχθηκαν άκυρες από το Ευρωπαϊκό Δικαστήριο τον Οκτώβριο του 2015.

Η Privacy Shield όπως και το Safe Harbour βασίστηκε σε ένα σύστημα αυτοπιστοποίησης με το οποίο οι αμερικανικοί οργανισμοί δεσμεύονταν να τηρήσουν ένα σύνολο αρχών προστασίας της ιδιωτικής ζωής. Ωστόσο, σε αντίθεση με το Safe Harbour που περιείχε μόνο μια γενική εξαίρεση για τους σκοπούς εθνικής ασφάλειας, η απόφαση για την ασπίδα προστασίας της ιδιωτικής ζωής περιλάμβανε ένα τμήμα σχετικά με την πρόσβαση και την χρήση των προσωπικών δεδομένων που διαβιβάζονται στο πλαίσιο της συμφωνίας από τις δημόσιες αρχές των ΗΠΑ για σκοπούς εθνικής ασφάλειας και επιβολής του νόμου. Σχετικά με αυτή την περίπτωση, η Επιτροπή διαπίστωσε ότι υπάρχουν κανόνες στις Ηνωμένες Πολιτείες που έχουν σχεδιαστεί για να περιορίσουν κάθε παρέμβαση για σκοπούς εθνικής ασφάλειας στο βαθμό που παραβιάζουν τα θεμελιώδη δικαιώματα των προσώπων των οποίων τα προσωπικά δεδομένα διαβιβάζονται από την ΕΕ στις ΗΠΑ, στο απολύτως αναγκαίο για την επίτευξη του εν λόγω νόμιμου στόχου[81]. Το συμπέρασμα αυτό βασίστηκε στις διαβεβαιώσεις που παρείχε το Γραφείο του Διευθυντή της Εθνικής Εποπτείας, του Υπουργείου Δικαιοσύνης των ΗΠΑ (παράρτημα VII) και του Υπουργού Εξωτερικών των ΗΠΑ (παράρτημα III), οι οποίες περιγράφουν τους περιορισμούς, την εποπτεία και τις δυνατότητες δικαστικής προσφυγής στο πλαίσιο των προγραμμάτων παρακολούθησης των ΗΠΑ (Tzanou, 2020).

Η Ασπίδα Προστασίας της Ιδιωτικής Ζωής ΕΕ-ΗΠΑ επιβάλει στις εταιρείες στις ΗΠΑ αυστηρές υποχρεώσεις για την προστασία των προσωπικών δεδομένων των ατόμων και πιο ισχυρό παρακολούθηση και επιβολή από το Υπουργείο Εμπορίου και την Ομοσπονδιακή Επιτροπή Εμπορίου (FTC), συμπεριλαμβανομένης της αυξημένης συνεργασίας με τις Ευρωπαϊκές Αρχές Προστασίας Δεδομένων. Η συμφωνία αυτή περιλαμβάνει γραπτές δεσμεύσεις και διαβεβαιώσεις από τις ΗΠΑ ότι κάθε πρόσβαση των δημοσίων αρχών σε προσωπικά δεδομένα που μεταφέρθηκαν στο νέο πλαίσιο για λόγους εθνικής ασφάλειας θα υπόκειται σε σαφείς προϋποθέσεις, περιορισμούς και εποπτεία, αποτρέποντας τη γενικευμένη πρόσβαση. Με το πλαίσιο αυτό ιδρύθηκε και ο μηχανισμός του Διαμεσολαβητή

[80] Εκτελεστική Απόφαση (ΕΕ) 2016/1250 της Επιτροπής της 12 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), διαθέσιμη στο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016D1250 (τελευταία προσπέλαση: 21 Απριλίου 2024)

[81] Privacy Shield, recital 88

που ασχολείται με την επίλυση παραπόνων ή ερωτήσεων που τίθενται από τα υποκείμενα της ΕΕ σε αυτό το πλαίσιο.

Έχουν εγερθεί σοβαρές ανησυχίες σχετικά με το κατά πόσον η Ασπίδα Προστασίας της ιδιωτικής ζωής συμμορφώνεται με τα πρότυπα της ΕΕ για την προστασία των δεδομένων και της ιδιωτικής ζωής. Σχετικώς, η Ομάδα Εργασίας του Άρθρου 29, εξέφρασε την ανησυχία του ότι οι προφορικές δεσμεύσεις των ΗΠΑ δεν επαρκούν για να συμβιβάσουν την ανεπάρκεια και την αδυναμία τους να παράσχουν ουσιαστικά ισοδύναμη προστασία βάσει της εθνικής νομοθεσίας[82]. Συγκεκριμένα, διαφώνησε ως προς το μηχανισμό του Διαμεσολαβητή, εντοπίζοντας ιδιαίτερη πολυπλοκότητα σε αυτό το σύστημα για την έγκαιρη αντιμετώπιση παραβιάσεων της προστασίας δεδομένων και των δικαιωμάτων ιδιωτικής ζωής. Η Επιτροπή στήριξε την ανάλυση επάρκειας της Ασπίδας Προστασίας της ιδιωτικής ζωής απλώς σε μια λεπτομερή περιγραφή του αμερικανικού δικαίου, χωρίς να έχουν αναληφθεί ουσιαστικές δεσμεύσεις (με εξαίρεση τον Διαμεσολαβητή) από τις ΗΠΑ, προκειμένου να συμμορφωθούν με τις απαιτήσεις της ΕΕ για τα θεμελιώδη δικαιώματα, όπως ορίζονται από την απόφαση του ΔΕΕ στην υπόθεση Schrems I. Η Ασπίδα Προστασίας της Ιδιωτικής Ζωής επικρίθηκε επίσης για την έλλειψη εποπτείας των προγραμμάτων παρακολούθησης των ΗΠΑ και την έλλειψη δικαστικής προσφυγής[83].

Το Δικαστήριο Ευρωπαϊκής Ένωσης κήρυξε άκυρη την Ασπίδα Προστασίας της Ιδιωτικής Ζωής ΕΕ-ΗΠΑ στις 16 Ιουλίου 2020, στην υπόθεση που είναι γνωστή ως Schrems II[84]. Στη Schrems II τα πραγματικά περιστατικά της υπόθεσης είναι ομοιάζουν σε μεγάλο βαθμό με αυτά της υπόθεσης Schrems I του 2016. Μετά την ακύρωση του ασφαλούς λιμένα, ο Max Schrems ζήτησε από την Αρχή Προστασίας Δεδομένων της Ιρλανδίας να αναστείλει τη μεταφορά των προσωπικών του δεδομένων που κατείχε το Facebook Ireland στη Facebook, Inc, τη μητρική του εταιρεία που εδρεύει στις ΗΠΑ, με το σκεπτικό ότι αυτά θα μπορούσαν να διατεθούν στις αρχές των ΗΠΑ, όπως η NSA και το Ομοσπονδιακό Γραφείο Ερευνών (FBI), στο πλαίσιο προγραμμάτων παρακολούθησης που παραβιάζουν τα δικαιώματα, που εγγυώνται τα άρθρα 7, 8 ΧΘΔ και 47 της ΣΕΕ (Tzanou, 2020).

Η αξίωση του Schrems σε αυτή την υπόθεση αφορούσε τη διαβίβαση δεδομένων στις ΗΠΑ στο πλαίσιο των τυποποιημένων συμβατικών ρητρών βάσει της απόφασης 2010/87[85].

---

[82] WP29, Opinion 1/2016 of 13 April 2016 on the EU–U.S. Privacy Shield draft adequacy decision WP 238; Resolution of the Parliament of 6 April 2017 on the adequacy of the protection afforded by the EU–US Privacy Shield, P8_TA(2017)0131, para 17;., διαθέσιμο στο https://ec.europa.eu/newsroom/article29/items/640157/en, (τελευταία προσπέλαση: 21 Απριλίου 2024)

[83] Βλ. WP29, EU–U.S. Privacy Shield – First Annual Joint Review, 28 November 2017, WP 255;
European Parliament Resolution of 5 July 2018 on the adequacy of the protection afforded by the EUUS Privacy Shield, P8_TA (2018)0315 (paragraph 22)

[84] Απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης της 16ης Ιουλίου 2020 στην υπόθεση C-311/18, στο πλαίσιο της δίκης Schrems κατά Facebook Ireland, διαθέσιμο στο https://curia.europa.eu/juris/liste.jsf?num=C-311/18

[85] Απόφαση της Επιτροπής της 5ης Φεβρουαρίου 2010 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [κοινοποιηθείσα υπό τον αριθμό Ε(2010) 593], διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32010D0087 (τελευταία προσπέλαση: 21 Απριλίου 2024)

Ως εκ τούτου, η Αρχή Προστασίας Δεδομένων της Ιρλανδίας διατύπωσε την άποψη ότι η αξιολόγηση της καταγγελίας του Schrems εξαρτιόταν από την εγκυρότητα της απόφασης 2010/87 και κίνησε διαδικασία ενώπιον του Ανωτάτου Δικαστηρίου της Ιρλανδίας και ζήτησε από αυτό να προβεί σε προδικαστική παραπομπή στο ΔΕΕ για να ζητήσει διευκρινίσεις σχετικά με το ζήτημα αυτό. Σε μία απόφαση-ορόσημο, που εκδόθηκε στις 16 Ιουλίου 2020, το ΔΕΕ έκρινε ότι η απόφαση 2010/87 παραμένει έγκυρη, ενώ ακύρωσε την Privacy Shield.

Στην εξέταση της Ασπίδας Προστασίας για την Ιδιωτικότητα, το ΔΕΕ εστίασε στη δέσμευση των ΗΠΑ στις αρχές της συμφωνίας. Η Privacy Shield ανέφερε σχετικώς ότι η τήρηση των αρχών από τις ΗΠΑ περιορίζεται στο βαθμό που είναι απαραίτητο για την εκπλήρωση των απαιτήσεων εθνικής ασφάλειας, δημόσιας ή επιβολής του νόμου. Συνεπώς, κάθε φορά που οι υποχρεώσεις για συμμόρφωση με την Privacy Shield έρχονταν σε σύγκρουση με την εθνική ασφάλεια, το δημόσιο συμφέρον ή τη νομοθεσία των ΗΠΑ για την επιβολή του νόμου, οι ΗΠΑ θα μπορούσαν να αγνοήσουν εντελώς την Ασπίδα Προστασίας της ιδιωτικής ζωής (Calia, 2022).

Η απόφαση Schrems II έχει σημαντικές θεωρητικές και πρακτικές προεκτάσεις, καθώς κατασκευάζει νέες απαιτήσεις για νομικούς μηχανισμούς για τις διασυνοριακές διαβιβάσεις δεδομένων εκτός από τις αποφάσεις επάρκειας, όπως για παράδειγμα τις τυποποιημένες συμβατικές ρήτρες. Επιπλέον, στην απόφαση του αυτή το ΔΕΕ κατάφερε να αναπτύξει καλύτερα το επίπεδο προστασίας που πράγματι επιτυγχάνει η Privacy Shield, καθώς και το επίπεδο που θα έπρεπε να διασφαλίζεται από το πλαίσιο αυτό, ενώ γίνεται προσεκτικότερη εξέταση του νομοθετικού πλαισίου των ΗΠΑ, σε σχέση με την απόφαση του ΔΕΕ στην υπόθεση Schrems I (Tzanou, 2020).

5.3.3 Το νέο πλαίσιο για τη μεταφορά δεδομένων μεταξύ ΕΕ και ΗΠΑ

Στις 10 Ιουλίου 2023 η Ευρωπαϊκή Επιτροπή εξέδωσε νέα Απόφαση Επάρκειας για ασφαλείς και έμπιστες ροές δεδομένων μεταξύ ΕΕ και ΗΠΑ[86]. Το πλαίσιο ΕΕ-ΗΠΑ για την προστασία των δεδομένων εισάγει σημαντικές νέες εγγυήσεις για την αντιμετώπιση όλων των προβληματισμών, που είχαν διατυπωθεί από το Δικαστήριο της Ευρωπαϊκής Ένωσης. Η πρόεδρος, κ. Ούρσουλα φον ντερ Λάιεν, δήλωσε σχετικά: «Το νέο πλαίσιο ΕΕ-ΗΠΑ για την προστασία των δεδομένων θα εξασφαλίσει ασφαλείς ροές δεδομένων για τους Ευρωπαίους και θα προσφέρει ασφάλεια δικαίου στις εταιρείες και στις δύο πλευρές του Ατλαντικού. Μετά την κατ' αρχήν συμφωνία που επετεύχθη πέρυσι με τον Πρόεδρο Μπάιντεν, οι ΗΠΑ υλοποίησαν πρωτοφανείς δεσμεύσεις για τη θέσπιση του νέου πλαισίου. Σήμερα κάνουμε ένα σημαντικό βήμα για να παράσχουμε στους πολίτες την εμπιστοσύνη ότι τα δεδομένα τους είναι ασφαλή, να εμβαθύνουμε τους οικονομικούς δεσμούς μεταξύ της ΕΕ και των ΗΠΑ και, ταυτόχρονα, να επιβεβαιώσουμε εκ νέου τις κοινές μας αξίες. Αποδεικνύεται ότι, μέσω της συνεργασίας, μπορούμε να αντιμετωπίσουμε και τα πλέον περίπλοκα ζητήματα[87].».

[86] Εκτελεστική απόφαση (ΕΕ) 2023/1795 της Επιτροπής της 10ης Ιουλίου 2023 σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επάρκεια του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα βάσει του πλαισίου ΕΕ-ΗΠΑ για την προστασία των δεδομένων, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32023D1795

[87] Δελτίο τύπου στην ιστοσελίδα της Ευρωπαϊκής Επιτροπής, https://ec.europa.eu/commission/presscorner/detail/el/ip_23_3721

Το Πλαίσιο ΕΕ–ΗΠΑ υιοθετεί ένα σύστημα πιστοποίησης των οργανισμών των ΗΠΑ, οι οποίο δεσμεύονται να τηρούν ένα σύνολο αρχών προστασίας της ιδιωτικής ζωής, τις αρχές του πλαισίου ΕΕ–ΗΠΑ για την προστασία των δεδομένων, συμπεριλαμβανομένων των συμπληρωματικών αρχών, οι οποίες εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ[88]. Μεταξύ των αρχών του Πλαισίου[89], περιλαμβάνονται η αρχή του περιορισμού του σκοπού, η αρχή της ακρίβειας και της ελαχιστοποίησης, η αρχή της διαφάνειας και η αρχή της λογοδοσίας. Αρμόδιο όργανο για την παρακολούθηση της συμμόρφωσης των οργανισμών με τις αρχές του Πλαισίου είναι το Υπουργείο Εμπορίου των ΗΠΑ μέσω διαφόρων μηχανισμών, όπως είναι οι «επιτόπιοι έλεγχοι»[90].

Αξιοσημείωτη είναι η πρόβλεψη του Πλαισίου αναφορικά με τον περιορισμό της πρόσβασης και χρήσης από δημόσιες αρχές των ΗΠΑ σε δεδομένα προσωπικού χαρακτήρα, που έχουν διαβιβαστεί από την ΕΕ σε ό,τι είναι αναγκαίο και αναλογικό[91], διακρίνοντας δύο περιπτώσεις: την πρόσβαση και χρήση για σκοπούς επιβολής της ποινικής νομοθεσίας[92] και την πρόσβαση και χρήση για σκοπούς εθνικής ασφάλειας[93]. Εξάλλου, σημαντική καινοτομία του Πλαισίου αποτελεί η δημιουργία ενός Δικαστηρίου Ελέγχου της Προστασίας Δεδομένων (Data Protection Review Court - DPRC), στο οποίο θα έχουν πρόσβαση άτομα από την ΕΕ, όσον αφορά τη συλλογή και τη χρήση δεδομένων από δημόσιες αρχές των ΗΠΑ για σκοπούς εθνικής ασφάλειας[94]. Το Δικαστήριο θα διερευνά και θα επιλύει ανεξάρτητα καταγγελίες, μεταξύ άλλων με τη λήψη δεσμευτικών διορθωτικών μέτρων. (Data Privacy Framework, 2023).

Η Αρχή Προστασίας Δεδομένων του Αμβούργου σημειώνει ότι, προς το παρόν, οι ΗΠΑ δεν έχουν επιτύχει ουσιαστικά ισοδύναμο επίπεδο προστασίας δεδομένων με αυτό της ΕΕ και επισημαίνει ότι δεν είναι σαφές από το κείμενο του Πλαισίου σε ποιο βαθμό η νέα απαίτηση αναλογικότητας ισχύει για τη μαζική επιτήρηση[95]. Σημειώνει επίσης ότι οι διαδικασίες προσφυγής δεν είναι διαφανείς και κατανοητές για τους καταγγέλλοντες[96].

Τον Φεβρουάριο του 2023, το EDPB εξέδωσε μία μη δεσμευτική γνώμη για το σχέδιο απόφασης επάρκειας[97]. Ειδικότερα, αναφέρει ότι «καλωσορίζει τις ουσιαστικές βελτιώσεις, αλλά ταυτόχρονα, εκφράζει ανησυχίες και ζητεί διευκρινίσεις σε πολλά σημεία […] ειδικότερα, σχετικά με ορισμένα δικαιώματα των υποκειμένων των δεδομένων, και σχετικά

[88] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 2.1.1 (9)
[89] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 2.2

[90] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 2.3.2 (53)
[91] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 3
[92] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 3.1
[93] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 3.2
[94] Εκτελεστική απόφαση (ΕΕ) 2023/1795, 3.2.3 (176)
[95] Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086, διαθέσιμο στο https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739261 (τελευταία προσπέλαση: 22 Απριλίου 2024)
[96] ό.π.
[97] EDPB Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, διαθέσιμο στο https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en

με τις περαιτέρω διαβιβάσεις, στο πεδίο εφαρμογής των εξαιρέσεων, την μαζική συλλογή των δεδομένων και σχετικά με την πρακτική λειτουργία του μηχανισμού επανόρθωσης.» (EDPB, 2023).

Συνοψίζοντας, στο κεφάλαιο αυτό κατέστησαν σαφείς οι προσπάθειες για τη δημιουργία ενός σαφούς και αυστηρού ρυθμιστικού πλαισίου αναφορικά με τη διασυνοριακή ροή δεδομένων. Οι περιφερειακές πρωτοβουλίες αποτέλεσαν τον βασικό μοχλό για τη ρύθμιση της διασυνοριακής ροής, ωστόσο ορισμένα πλαίσια εξακολουθούν να βασίζονται σε εθελοντικές αρχές και σε πρότυπα και η σημασία τους σήμερα μειώνεται. Παρόλο που οι γενικές αρχές και τα πρότυπα αυτά παρέχουν πολύ χρήσιμη καθοδήγηση, σήμερα προτεραιότητα θα πρέπει να είναι η εφαρμογή και η επιβολή (και, όπου είναι δυνατόν, η εναρμόνιση) των νομοθεσιών. Στο πλαίσιο της Ευρωπαϊκής Ένωσης, ακολουθείται ένα αυστηρό πρότυπο, όπου οι διαβιβάσεις των προσωπικών δεδομένων εκτός της εδαφικής της κυριαρχίας γίνεται υπό συγκεκριμένες προϋποθέσεις, και ιδίως εφόσον η χώρα έχει επαρκές επίπεδο προστασίας των δεδομένων και υφίσταται αντίστοιχη απόφαση της Επιτροπής, ή εφόσον η εταιρεία που διαβιβάζει τα δεδομένα παρέχει κατάλληλες εγγυήσεις μέσω μηχανισμών όπως, δεσμευτικών εταιρικών κανόνων (BCR), τυποποιημένων συμβατικών ρητρών προστασίας δεδομένων ή εγκεκριμένου κώδικα δεοντολογίας.

Συμπεράσματα

Σε ένα παγκοσμιοποιημένο ψηφιακό τοπίο, όπου η διασυνοριακή διαβίβαση δεδομένων αποτελεί συνήθη πρακτική, καθίσταται επιτακτική η ομοιόμορφη πρακτική των κρατών αναφορικά με την προστασία των προσωπικών δεδομένων. Αφετηρία για την προσπάθεια δημιουργίας ενός ενιαίου διεθνούς προτύπου για την προστασία προσωπικών δεδομένων αποτέλεσαν η ΕΣΔΑ καθώς και τα κείμενα του ΟΟΣΑ και του Συμβουλίου της Ευρώπης. Οι βασικές αρχές και ορισμένες ρυθμίσεις των κειμένων αυτών έχουν αποκρυσταλλωθεί στις νομοθεσίες των κρατών παγκοσμίως και ισχύουν έως σήμερα.

Αδιαμφισβήτητα, η Ευρωπαϊκή Ένωση έχει πρωτοστατήσει στη διαμόρφωση ενός ολοκληρωμένου και αυστηρού πλαισίου για την προστασία προσωπικών δεδομένων. Κομβικό σημείο αποτέλεσε η υιοθέτηση του GDPR, σε μία περίοδο όπου η συνεχής τεχνολογική εξέλιξη προξένησε πολλαπλούς κινδύνους για την ιδιωτικότητα, ενώ ταυτόχρονα η συλλογή δεδομένων εμφανιζόταν ολοένα και πιο ελκυστική τόσο για εμπορικούς σκοπούς, αλλά ακόμη και τη χειραγώγηση των ατόμων για πολιτικούς σκοπούς.

Η επιρροή του αυστηρού ενωσιακού προτύπου για την προστασία πολύ σύντομα ξεπέρασε τα εδαφικά όρια των κρατών μελών της Ευρωπαϊκής Ένωσης. Μετά την υιοθέτηση του GDPR, πολλά κράτη διεθνώς διαμόρφωσαν για πρώτη φορά αντίστοιχα νομικά πλαίσια, ή αναθεώρησαν το υπάρχουν νομικό τους καθεστώς σύμφωνα με το πρότυπο της ΕΕ. Το φαινόμενο αυτό, γνωστό ως «Brussels Effect», δεν έχει μία προφανή εξήγηση, αλλά οφείλεται σε πολλαπλούς παράγοντες με βασική αιτία την επιθυμία των εταιριών να δραστηριοποιούνται στην αγορά της ΕΕ και την αντίστοιχη πίεση των εταιριών αυτών προς τα θεσμικά όργανα να υιοθετήσουν αντίστοιχο με την ΕΕ νομικό καθεστώς.

Σημαντικό τροχοπέδη στην υιοθέτηση ομοιόμορφου νομοθετικού προτύπου για την αντιμετώπιση της απειλής της ιδιωτικότητας αποτελεί η προσέγγιση του ζητήματος από την πλευρά των ΗΠΑ. Στις ΗΠΑ, η προσέγγιση για την προστασία της ιδιωτικής ζωής και των δεδομένων εξακολουθεί να συνίσταται σε ένα συνονθύλευμα πολιτειακών και ομοσπονδιακών νόμων, ενώ δεν υπάρχει ένα ολοκληρωμένο γενικό πλαίσιο. Ως εκ τούτου, η προστασία των υποκειμένων από την επεξεργασία των προσωπικών τους δεδομένων διαφέρει από τον ένα τομέα δραστηριότητας στον άλλον και από τη μία Πολιτεία στην άλλη. Ο πιο ολοκληρωμένος και σαφής νόμος θεωρείται ο California Consumer Privacy Act (CCPA), ο οποίος, αν και ομοιάζει σημαντικά με τον GDPR, παρουσιάζει και αρκετές διαφοροποιήσεις.

Επισημαίνεται ότι άλλα κράτη που είχαν όμοια προσέγγιση με τις ΗΠΑ, όπως η Κίνα και η Βραζιλία, έχουν πλέον ακολουθήσει το παράδειγμα της ΕΕ, λίγα χρόνια μετά την έναρξη ισχύος του GDPR. Στο πλαίσιο αυτό, οι ΗΠΑ βρίσκονται πιο κοντά από ποτέ να υιοθετήσουν έναν ολοκληρωμένο ομοσπονδιακό νόμο για την προστασία προσωπικών δεδομένων.

Στις 7 Απριλίου 2024, η Αμερικανίδα εκπρόσωπος Cathy Rodgers και η Αμερικανίδα γερουσιαστής Maria Cantwell παρουσίασαν το νομοσχέδιο American Privacy Rights Act (APRA) 2024, το οποίο εφόσον ψηφιστεί πρόκειται να θεσπίζει το δικαίωμα στην προστασία της ιδιωτικής ζωής και των δεδομένων των καταναλωτών και θα θέτει πρότυπα για την ασφάλεια των δεδομένων. Το νομοσχέδιο έχει διακομματική υποστήριξη και είναι το πρώτο

ολοκληρωμένο ομοσπονδιακό νομοσχέδιο για την προστασία της ιδιωτικής ζωής στις ΗΠΑ που παρουσιάζεται μετά τον Αμερικανικό νόμο για την προστασία της ιδιωτικής ζωής και την προστασία των δεδομένων (American Data Privacy and Protection Act - ADPPA).

Το νομοσχέδιο δεν ορίζει ρητά το πεδίο εφαρμογής αυτού, αλλά διευκρινίζει τις οντότητες και τα δεδομένα στα οποία θα εφαρμόζεται. Για το σκοπό αυτό, το νομοσχέδιο ορίζει ως «καλυπτόμενα δεδομένα»: τις πληροφορίες που ταυτοποιούν ή συνδέονται ή μπορούν ευλόγως να συνδεθούν, μόνες τους ή σε συνδυασμό με άλλες πληροφορίες, με ένα άτομο ή μια συσκευή που ταυτοποιεί ή συνδέεται ή μπορεί ευλόγως να συνδεθεί με ένα ή περισσότερα άτομα. Αξίζει να σημειωθεί ότι το νομοσχέδιο περιγράφει λεπτομερώς διάφορα είδη δεδομένων που δεν θα ταξινομούνται ως καλυπτόμενα δεδομένα, συμπεριλαμβανομένων των ανώνυμων δεδομένων, των πληροφοριών των εργαζομένων και των δημοσίως διαθέσιμων πληροφοριών[98]. Σε σχέση με τις οντότητες που θα υπόκεινται στο νομοσχέδιο, το νομοσχέδιο ορίζει ως «καλυπτόμενη οντότητα»: κάθε οντότητα που, μόνη της ή από κοινού με άλλους, καθορίζει τους σκοπούς και τα μέσα συλλογής, επεξεργασίας, διατήρησης ή διαβίβασης καλυπτόμενων δεδομένων- και υπόκειται στον νόμο της Ομοσπονδιακής Επιτροπής Εμπορίου[99]. Αξιοσημείωτο είναι ότι στην έννοια της «καλυπτόμενης οντότητας» δεν εμπίπτει οποιαδήποτε ομοσπονδιακή, πολιτειακή, ή τοπική κυβερνητική οντότητα, αλλά ούτε και οντότητες που συλλέγουν, επεξεργάζονται, διατηρούν ή διαβιβάζουν καλυπτόμενα δεδομένα για λογαριασμό των ανωτέρω οντοτήτων, όταν ενεργούν ως πάροχοι υπηρεσιών προς την κυβερνητική οντότητα. Τέλος, το νομοσχέδιο δεν αφορά ούτε τις μικρές επιχειρήσεις[100].

Το νομοσχέδιο απαγορεύει στις καλυπτόμενες οντότητες και στους παρόχους υπηρεσιών να προβαίνουν στη συλλογή, επεξεργασία, διατήρηση ή διαβίβαση καλυπτόμενων δεδομένων στο βαθμό που αυτή δεν είναι αναγκαία, αναλογική και περιορισμένη για την παροχή ή διατήρηση συγκεκριμένου προϊόντος ή υπηρεσίας που ζητείται από το άτομο ή μιας επικοινωνίας που εύλογα αναμένεται στο πλαίσιο της σχέσης, ή γίνεται για σκοπό διαφορετικό από τον «επιτρεπόμενο σκοπό»[101]. Το νομοσχέδιο παρέχει μεγαλύτερη προστασία για τις ευαίσθητες, βιομετρικές και γενετικές πληροφορίες, απαιτώντας τη θετική ρητή συγκατάθεση για τη συλλογή, την επεξεργασία, τη διατήρηση ή τη διαβίβαση ευαίσθητων πληροφοριών σε τρίτου[102]. Όσον αφορά τη ρητή συγκατάθεση, το νομοσχέδιο ορίζει ότι η καλυπτόμενη οντότητα πρέπει να παρέχει στο άτομο τη δυνατότητα ανάκλησης της ρητής συγκατάθεσης με μηχανισμό σαφή, εμφανή και εξίσου εύκολο με αυτόν που παρέχει το άτομο τη συγκατάθεσή σου[103].

Εξάλλου, το νομοσχέδιο παρέχει στους καταναλωτές το δικαίωμα πρόσβασης, διόρθωσης, διαγραφής και φορητότητας των καλυπτόμενων δεδομένων. Όσον αφορά τα απλά δεδομένα, το νομοσχέδιο εισάγει το δικαίωμα εξαίρεσης από τη διαβίβαση μη ευαίσθητων καλυπτόμενων δεδομένων και τη στοχευμένη διαφήμιση. Για το σκοπό αυτό, η

[98] APRA, section 101 (12)
[99] APRA, section 101 (13, A)
[100] APRA, section 101 (13, C)
[101] APRA, section 102 (A)
[102] APRA, section 102
[103] APRA, section 101

καλυπτόμενη οντότητα πρέπει να παρέχει στο άτομο σαφή και ευδιάκριτο μηχανισμό για να εξαιρεθεί και να συμμορφώνεται με κάθε τέτοια δήλωση εξαίρεσης που γίνεται από ένα άτομο και να την κοινοποιεί σε όλους τους σχετικούς παρόχους υπηρεσιών[104]. Σύμφωνα με το νομοσχέδιο, αρμόδια αρχή για την επιβολή των διατάξεών του είναι η Federal Trade Commission, με τη σύσταση ενός γραφείου εντός της FTC, το οποίο θα παράσχει βοήθεια στην FTC κατά την άσκηση των αρμοδιοτήτων της βάσει του νομοσχεδίου και των συναφών αρχών[105].

Η ψήφιση του νομοσχεδίου, εφόσον αυτή λάβει χώρα, θα αποτελέσει σημείο καμπής για την προστασία προσωπικών δεδομένων, όχι μόνο για τις Ηνωμένες Πολιτείες, αλλά κυρίως για την διακρατική προσπάθεια αντιμετώπισης του ζητήματος. Είναι επιτακτική ανάγκη να υπάρχει ένα σαφές και αυστηρό ρυθμιστικό πλαίσιο για τη διασυνοριακή ροή δεδομένων. Η διαχείριση της παγκόσμιας διακίνησης πληροφοριών δημιουργεί συνεχείς προκλήσεις όσον αφορά την προστασία της ιδιωτικής ζωής, την ασφάλεια και τον έλεγχο των δεδομένων. Στη σημερινή καινοτόμο οικονομία, βασιζόμαστε όλο και περισσότερο στη διασυνοριακή ανταλλαγή δεδομένων για την επικοινωνία και τη συλλογή πληροφοριών. Ιδίως για τις επιχειρήσεις, η διασυνοριακή μεταφορά δεδομένων είναι σημαντική για την επέκταση της εμβέλειάς τους και τη σύνδεση με πελάτες σε νέες αγορές.

Καθώς η χρήση των δεδομένων στην τεχνολογία εξελίσσεται, οι κυβερνήσεις και οι επιχειρήσεις πρέπει να συνεργαστούν για να διασφαλίσουν ότι τα διασυνοριακά δεδομένα ρυθμίζονται με τρόπο που προωθεί την καινοτομία, προστατεύει την ιδιωτική ζωή και την ασφάλεια και σέβεται την εθνική κυριαρχία. Η ρύθμιση αυτών των διεθνών ροών δεδομένων αποτελεί αμφιλεγόμενο ζήτημα στις διεθνείς εμπορικές διαπραγματεύσεις, με τις χώρες να προσπαθούν να εξισορροπήσουν τα οφέλη της ροής δεδομένων με την ανάγκη προστασίας της ιδιωτικής ζωής και της ασφάλειας των πολιτών τους.

Η υιοθέτηση ενός ολοκληρωμένου εθνικού νόμου στις ΗΠΑ για την προστασία της ιδιωτικής ζωής αποτελεί ζήτημα μείζονος σημασίας, αφενός προκειμένου να καταστεί εφικτό στους πολίτες των ΗΠΑ να ελέγχουν τις προσωπικές τους πληροφορίες εντός των 50 πολιτειών, αφετέρου για να διευκολύνει την δραστηριοποίηση των αμερικανικών εταιριών εκτός αμερικανικών συνόρων και εν γένει να διαφυλάξει την ασφαλή διασυνοριακή ροή δεδομένων. Καθώς περιηγούμαστε σε ένα ολοένα και πιο περίπλοκο ψηφιακό περιβάλλον, είναι επιτακτική η ανάγκη για την υιοθέτηση παγκοσμίως ενός ισχυρού, τυποποιημένου πλαισίου για τη ρύθμιση της χρήσης των δεδομένων των υποκειμένων, το οποίο θα εστιάζει στη διαφάνεια και θα επιτρέπει τον έλεγχο των δεδομένων από τα ίδια τα υποκείμενα.

[104] APRA, section 106

[105] APRA, section 115

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ΕΛΛΗΝΟΓΛΩΣΣΗ

Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία (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), Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 1/2016

Γεωργίλη Ελίνα (2022), Cloud computing και διαβιβάσεις δεδομένων στις Η.Π.Α., Συνήγορος, 153/2022

Δημητρακοπούλου Κωνσταντίνα (2022), Δίκαιο εκτός ΕΕ – Σύγκριση του δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα της ΕΕ με εκείνο των ΗΠΑ, Κυπριακή Νομική Επιθεώρηση, 2/2022

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (2023), Γνώμη 5/2023 σχετικά με το σχέδιο εκτελεστικής απόφασης της Ευρωπαϊκής Επιτροπής για την επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα βάσει του πλαισίου προστασίας δεδομένων ΕΕ-ΗΠΑ, διαθέσιμο στο https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_el.pdf

Ιγγλεζάκης Ιωάννης (2020), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων: Κανονισμός 2016/679 και ο Εφαρμοστικός Νόμος Ν. 4624/2019, 3η εκδ., Interactive Books

Κανέλλος Λεωνίδας (2020), The GDPR Handbook, Νομική Βιβλιοθήκη

Μήτρου Λίλιαν (2017), Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων: Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα, Εκδόσεις Σάκκουλα

Παπαδοπούλου Ευγενία (2021), Η αξιολόγηση πιστοληπτικής ικανότητας στο δίκαιο προστασίας προσωπικών δεδομένων ΗΠΑ και ΕΕ, Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 1/2021

Τάσσης Σπύρος (2015), Σημείωμα στην ΔΕΕ υπόθ. C-362/14, απόφ. της 6.10.2015 - ΟΙ ΗΠΑ δεν αποτελούν πλέον «ασφαλές λιμάνι» για τα προσωπικά δεδομένα των πολιτών της ΕΕ, Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, 3/2015

Τάσσης Σπύρος (2021), Σχόλιο στην ΔΕΕ υπόθ. C-311/18, απόφ. της 15.9.2020 - Διασυνοριακή διαβίβαση δεδομένων στις ΗΠΑ μετά την Schrems II, Εφαρμογές Δημοσίου Δικαίου, 2-3/2021

Χριστοδούλου Κωνσταντίνος (2020), Δίκαιο Προσωπικών Δεδομένων, 2η εκδ., Νομική Βιβλιοθήκη

2. ΞΕΝΟΓΛΩΣΣΗ

Abraham L Newman (2008), Protectors of Privacy: Regulating Personal Data in the Global Economy, Cornell University Press

Amdahl Stephany (2023), The European Union's GDPR and Data Protection Law in the U.S. and China, Norwegian University of Science and Technology, Bachelor's Thesi.,/s, διαθέσιμο στο https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3072527

Arroyo Veronica, Hess Karin, Grunbaum Nicole & Ribeiro Gustavo (2023), What specific measures could the US, the EU and China take in order to foster and facilitate cross-border data flows?, Students Policy Brief, διαθέσιμο στο https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/09/policy-brief-data-flows.pdf

ASEAN (2018), ASEAN Framework on Digital Data Governance, διαθέσιμο στο 6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf

ASEAN (2021), ASEAN Data Management Framework, https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf

ASEAN (2021), ASEAN Model Contractual Clauses for Cross Border Data Flows, https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf

Bach David and Newman Abraham L (2007), The European Regulatory State and Global Public Policy: Micro-Institutions, MacroInfluence, 14 Journal of European Public Policy, διαθέσιμο στο https://www.researchgate.net/publication/241610698_The_European_Regulatory_State_and_Global_Public_Policy

Bendiek Annegret & Stuerzer Isabella (2023), The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate, Digital Society, Volume 2, No. 5, διαθέσιμο στο https://pubmed.ncbi.nlm.nih.gov/36713889/

Bendiek Annegret & Romer Magnus (2019), Externalizing Europe: the global effects of European data protection, Digital Policy Regulation and Governance, Volume 21, No 1, διαθέσιμο στο https://www.econstor.eu/bitstream/10419/210482/1/Full-text-article-Bendiek-et-al-Externalizing-Europe.pdf

Bennett J Colin (1992), Regulating Privacy. Data Protection and Public Policy in Europe and the United States, Cornell University Press

Bignami Francesca (2020), Schrems II: The Right to Privacy and the New Illiberalism, Verfassungsblog on Matters Constitutional, διαθέσιμο στο https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/

Boyne Shawn (2018), Data Protection in the United States: U.S. National Report, Indiana University Robert H. McKinney School of Law Research Paper No. 11, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089004

Bradford Anu (2012), The Brussels Effect, Columbia Law and Economics Working Paper No. 533, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770634

Bradford Anu (2014), Exporting Standar ting Standards: The Externalization of the EU' ds: The Externalization of the EU's Regulat s Regulatory Power via Markets, International Review of Law and Economics, Volume 42, No 5, διαθέσιμο στο

https://www.researchgate.net/publication/266562131_Exporting_Standards_The_Externalization_of_the_EU's_Regulatory_Power_via_Markets

Brandeis Louis & Warren Samuel (1890), The Right to Privacy, Harvard Law Review 193, διαθέσιμο στο https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Bygrave Lee (2010), Privacy and Data Protection in an International Perspective, Oxford University Press, διαθέσιμο στο https://scandinavianlaw.se/pdf/56-8.pdf

Bygrave Lee (2020), The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, Computer Law & Security Review 40, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3617871

Cadwalladr Carole & Graham-Harrison Emma (2018), Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach διαθέσιμο στο https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cain Rita (1993), Don't Reach Out and Touch Us Any More: Expanding Telephone Consumer Protection, Journal of Direct Marketing, Volume 7, No. 1

Calia Donna (2022), Schrems II: The EU'S Influence on U.S. Data Protection and Privacy Laws, Washington University Global Studies Law Review, Volume 21, Issue 2, διαθέσιμο στο https://journals.library.wustl.edu/globalstudies/article/id/8750/

Casalini Francesca & González Javier Lopez (2019), Trade and cross-border data flows, OECD Trade Policy Papers, No. 220, OECD Publishing, διαθέσιμο στο https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1717572897&id=id&accname=guest&checksum=2C37B213EF0101E962BA8522A93FB11A

Cécile de Terwangne (2021), Council of Europe convention 108+: A modernized international treaty for the protection of personal data, Computer Law & Security Review, Volume 40, διαθέσιμο στο https://www.sciencedirect.com/science/article/abs/pii/S0267364920301023

Cécile de Terwangne (2022), Privacy and data protection in Europe: Council of Europe's Convention 108+ and the European Union's GDPR, Centre de Recherche Information, Droit et Societe, Namur Digital Institute, διαθέσιμο στο https://researchportal.unamur.be/en/publications/privacy-and-data-protection-in-europe-council-of-europes-conventi

Chin Yik-Chan & Zhao Jingwu (2022), Governing Cross-Border Data Flows: International Trade Agreements and Their Limits, Laws, Volume 11, No. 63, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4225990

Council of Europe (2018), Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Daniel Nicola F. (2022), EU Data Governance: Preserving Global Privacy in the Age of Surveillance, Johns Hopkins University (Doctoral Dissertation), διαθέσιμο στο https://jscholarship.library.jhu.edu/items/ad14097b-ec61-468a-ad73-ee7113103e48

Data Privacy Framework (2023), The United States and the European Union Begin Implementation of the European Union-U.S, American Journal of International Law, 117(2), pp. 346–352, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/united-states-and-the-european-union-begin-implementation-of-the-european-unionus-data-privacy-framework/CE8FA1259AE3FC142168F6F8C8E4134B

Dipersio Denise (2022), Data Protection, Privacy and US Regulation, European Language Resources Association, διαθέσιμο στο https://aclanthology.org/2022.legal-1.3.pdf

European Data Protection Board (2018), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, διαθέσιμο στο https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

European Data Protection Board (2022), Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), διαθέσιμο στο https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/recommendations-12022-application-approval-and_en

European Data Protection Board (2023), Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, διαθέσιμο στο https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en

Fefer Rachel (2020), Data Flows, Online Privacy, and Trade Policy, Congressional Research Service, διαθέσιμο στο https://sgp.fas.org/crs/row/R45584.pdf

Feys Meagali (2022), Is Canada's Proposed Consumer Privacy Protection Act Too High Risk Compared to E.U. Data Protection Law?, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4197313

Field Elizabeth (2020), United States Data Privacy Law: The Domino Effect After the GDPR, North Carolina Banking Institute, Volume 24, Issue 1, διαθέσιμο στο https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1514&context=ncbi

Gerke Sara & Rezaeikhonakdar Delaram (2022), Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps, Intelligence-Based Medicine 6, διαθέσιμο στο https://www.sciencedirect.com/science/article/pii/S266652122200014X

Gidron Tamar (2012), Privacy protection as a case study in personal rights protection in Israeli law, Computer Law & Security Review 28, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2159656

Glancy Dorothy (1979), The Invention of the Right to Privacy, Arizona Law Review, Volume 21, No. 1, διαθέσιμο στο https://digitalcommons.law.scu.edu/facpubs/317/

Goldsmith Jack and Wu Tim (2006), Who Controls the Internet? Illusions of a Borderless World, Oxford University Press, διαθέσιμο στο https://scholarship.law.columbia.edu/books/175/

Greenleaf Graham (2012), The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108, International Data Privacy Law 68, 77

Greenleaf Graham (2014), Asian Data Privacy Laws: Trade and Human Rights Perspectives, Oxford University Press

Greenleaf Graham (2018), Convention 108+ and the Data Protection Framework of the EU, University of New South Wales Law Research Series, Paper No. 18-19, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606

Greenwald Glenn and MacAskill Ewen (2013), NSA Prism program taps in to user data of Apple, Google and others, The Guardian, διαθέσιμο εδώ https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Guasch J. Luis & Hahn Robert W. (1999), The Costs and Benefits of Regulation: Implications for Developing Countries, The World Bank Research Observer, vol 14, no. 1, διαθέσιμο στο https://documents1.worldbank.org/curated/es/763951468315327580/pdf/766270JRN0WBRO00Box374385B00PUBLIC0.pdf

Gunst Simon & Ferdi de Ville (2021), The Brussels Effect: How the GDPR Conquered Silicon Valley, European Foreign Affairs Review, Volume 26, Issue 3, διαθέσιμο στο https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036

Haber Eldar & Tamo-Larrieux Aurelia (2020), Privacy and security by design: Comparing the EU and Israeli approaches to embedding privacy and security, Computer Law & Security Review 37, διαθέσιμο στο https://www.sciencedirect.com/science/article/abs/pii/S0267364920300145

Hoang Carolyn (2012), In the Middle: Creating a Middle Road Between U.S. and EU Data Protection Policies, Journal of the National Association of Administrative Law Judiciary, Volume 32, Issue 2, διαθέσιμο στο https://digitalcommons.pepperdine.edu/naalj/vol32/iss2/10/

Holvast Jan (2009), History of Privacy, IFIP Advances in Information and Communication Technology, Volume 298, διαθέσιμο στο https://link.springer.com/chapter/10.1007/978-3-642-03315-5_2

Hoofnagle Chris, Bart van der Sloot & Borgesius Frederik (2019), The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, Volume 28, No. 1, διαθέσιμο στο https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501

Hornuf Lars, Mangold Sonja & Yang Yayun (2023), Data Privacy and Crowdsourcing: A Comparison of Selected Problems in China, Germany and the United States, Springer Nature, διαθέσιμο στο https://link.springer.com/book/10.1007/978-3-031-32064-4

Horowitz Irving (2006), Privacy, publicity and security: the American context: Privacy is not only a right but also an obligation, EMBO reports No. 40-44, διαθέσιμο στο https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490299/

Hui Marsha, Laribee Stephen & Hogan Stephen (2002), Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues, Tulsa Journal of Comparative and International Law, Volume 9, Issue 2, διαθέσιμο στο https://digitalcommons.law.utulsa.edu/cgi/viewcontent.cgi?article=1087&context=tjcil

Jaar Dominic & Zeller Patrick (2009), Canadian Privacy Law: The Personal Information Protection and Electronic Documents Act (PIPEDA), International In-house Counsel Journal Vol. 2, No. 7, διαθέσιμο στο https://www.iicj.net/subscribersonly/09june/iicj4jun-dataprotection-patrickzeller-guidancesoftware-USA.pdf

Janger Edward & Schartz Paul (2002), The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules, Minnesota Law Review 1227, διαθέσιμο στο https://scholarship.law.umn.edu/mlr/1227/

Jonatas de Souza, Abe Jair, Luiz de Lima & Nilson de Souza (2020), The Brazilian Law on Personal Data Protection, International Journal of Network Security & Its Applications (IJNSA) Volume 12, No.6, διαθέσιμο στο https://www.researchgate.net/publication/347583331_The_Brazilian_Law_on_Personal_Data_Protection

Jonathan Sobel (2008), The Evolution of Data Protection as a Privacy Concern, and the Contract Law Dynamics Underlying It, Securing Privacy in the Internet Age 55

Juliussen Bjork, Kozyri Elisavet, Johansen Dag & Rui Jon (2023), The third country problem under the GDPR: enhancing protection of data transfers with technology, International Data Privacy Law, Volume 13, Issue 3, διαθέσιμο στο https://academic.oup.com/idpl/article/13/3/225/7226249

Kelly Charlsey (2022), Data Privacy Regulations in the United States, China, and the European Union, Georgia Southern University, Honors College Theses, 756, διαθέσιμο στο https://digitalcommons.georgiasouthern.edu/honors-theses/756/

Kinikoglu Batu (2023), Implementing a new data protection law: lessons from the Turkish experience, International Data Privacy Law, 2023, Volume 13, No. 1, διαθέσιμο στο https://academic.oup.com/idpl/article/13/1/25/7025584

Kong Lingjie (2010), Data Protection and Transborder Data Flow in the European and Global Context, The European Journal of International Law, Volume 21, No. 2, διαθέσιμο στο https://academic.oup.com/ejil/article/21/2/441/374186

Kramer Jay & Hoar Sean (2017), GDPR, Part I: History Of European Data Protection Law, διαθέσιμο στο https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf

Kuner Christopher (2011), Regulation of Transborder Data Flows under Data Protection and Privacy Law; Past, Present and Future, OECD Digital Economy Paper No. 187, OECD Publishing,

διαθέσιμο στο http://www.kuner.com/my-publications-and-writing/untitled/kuner-oecd-tbdf-paper.pdf

Kuner Christopher (2013), Transborder data flows and data privacy law, Oxford University Press

Kuner Christopher (2017), Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal, Volume 18, No. 4, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346

Lydia de la Torre (2018), A guide to the California Consumer Privacy Act of 2018, Santa Clara University, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275571

Lynskey Orla (2014), Deconstructing Data Protection: The 'Added value' of a right to data protection in the EU legal order, International and Comparative Law Quarterly 63(3), διαθέσιμο στο https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/abs/deconstructing-data-protection-the-addedvalue-of-a-right-to-data-protection-in-the-eu-legal-order/95BD4CCF4670466FD4F6EBAD7DDB4E76

Lynskey Orla (2020), Extraterritorial Impact in Data Protection Law through an EU Law Lens, Brexit Institute Working Paper Series, No 8, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3674413

Mattoo Aaditya & Meltzer Joshua (2018), International Data Flows and Privacy The Conflict and Its Resolution, Policy Research Working Paper 8431, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175036

Meltzer Joshua (2014), The Internet, Cross-Border Data Flows and International Trade, Asia & the Pacific Policy Studies, Volume 2, No. 1, διαθέσιμο στο https://onlinelibrary.wiley.com/doi/full/10.1002/app5.60

Mishra Neha (2019), Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows, NUS Centre for International Law Research Paper No. 19, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263271

Miyashita Hiroshi (2020), Human-centric Data Protection Laws and Policies: A Lesson from Japan, Computer Law & Security Review 40, διαθέσιμο στο https://www.researchgate.net/publication/346212467_Human-centric_data_protection_laws_and_policies_A_lesson_from_Japan

Moore Wilnellys & Frye Sarah (2019), Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules, Journal of Nuclear Medicine Technology, Volume 47, No 4, διαθέσιμο στο https://tech.snmjournals.org/content/jnmt/47/4/269.full.pdf

Moreira Hugo (2023), Governing Knowledge and Technology: Technological Pressure for Convergence in EU, California, and China Data Protection Regulation, CIES

Mostert Menno, Bredenoord L.Annelien, Bart van der Sloot & Johannes J.M. van Delden (2018), From Privacy to Data Protection in the EU: Implications for Big Data Health Research, European Journal of Health Law 25, 43-55, διαθέσιμο στο https://bartvandersloot.com/onewebmedia/From%20privacy%20to%20Data%20Protection.pdf

OECD (1980), Guidelines governing the protection of privacy and transborder flows of personal data, διαθέσιμο στο https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en

OECD (2013), Guidelines governing the protection of privacy and transborder flows of personal data, διαθέσιμο στο https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf

OECD (2022), Fostering Cross Border Data Flows With Trust, OECD Digital Economy Papers No. 343, διαθέσιμο στο https://www.oecd.org/science/fostering-cross-border-data-flows-with-trust-139b32ad-en.htm

Pardau Stuart (2018), The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States, Journal of Technology Law & Policy, Volume 23, Issue 1, διαθέσιμο στο https://scholarship.law.ufl.edu/jtlp/vol23/iss1/2/

Park Grace (2020), The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act, UC Irvine Law Review, Volume 10, Issue 4, διαθέσιμο στο https://scholarship.law.uci.edu/ucilr/vol10/iss4/11/

Pernot – Leplay Emmanuel (2020), China's Approach on Data Priv oach on Data Privacy Law: A Thir acy Law: A Third Way Between the y Between the U.S. and the E.U.?, Penn State Journal of Law & International Affairs, Volume 8, Issue 1, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542820

Peukert Christian, Bechtold Stefan, Batikas Michail & Kretschmer (2022), Regulatory Spillovers and Data Governance: Evidence from the GDPR, Marketing Science, Volume 41, No. 4, διαθέσιμο στο https://pubsonline.informs.org/doi/10.1287/mksc.2021.1339

Princen Sebastiaan (1999), The California Effect in the EC's External Relations: A Comparison of the Leghold Trap and the Beef-Hormone Issues Between the EC and the US & Canada, διαθέσιμο στο http://aei.pitt.edu/2367/

Proser William (1960), Privacy, California Law Review, Volume 48, No. 3, διαθέσιμο στο https://lawcat.berkeley.edu/record/1109651?v=pdf

Purtova Nadezhda (2018), The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, Volume 10, No. 1, διαθέσιμο στο https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

Roos Anneliese (2016), African Data Privacy Laws, Law, Governance and Technology Series 33, διαθέσιμο στο https://www.academia.edu/80425112/Data_Protection_Law_in_South_Africa

Rotenberg Marc (2020), Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection, European Law Journal, Volume 26, Issue 1-2, διαθέσιμο στο https://onlinelibrary.wiley.com/doi/abs/10.1111/eulj.12370

Ruben de Bruin (2022), A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence, Hastings Science and Technology Law Journal, Volume 13, No. 2, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251540

Rustad Michael & Koeing Thomas (2019), Towards a Global Data Privacy Standard, Florida Law Review, Volume 71, Issue 2, διαθέσιμο στο https://scholarship.law.ufl.edu/flr/vol71/iss2/3/

Ryngaert Cedric & Taylor Mistale (2020), Symposium on the GDPR and Internation Law: The GDPR as Global Data Protection Regulation?, AJIL Unbound 114, διαθέσιμο στο https://www.researchgate.net/publication/338406505_The_GDPR_as_Global_Data_Protection_Regulation

Safari Beata (2017), Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, Seton Hall Law Review, Volume 47, Issue 3, διαθέσιμο στο https://scholarship.shu.edu/shlr/vol47/iss3/6/

Solove Daniel (2006), A Brief History of Information Privacy Law, Proskauer on Privacy, διαθέσιμο στο https://scholarship.law.gwu.edu/faculty_publications/923/

Solove Daniel (2006), A taxonomy of privacy, University of Pennsylvania Law Review, Vol. 154/3, διαθέσιμο στο https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/

Schwartz Paul (2013), The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures, Harvard Law Review, Volume 126, διαθέσιμο στο https://harvardlawreview.org/print/vol-126/the-eu-u-s-privacy-collision-a-turn-to-institutions-and-procedures/

Schwartz Paul & Solove Daniel (2014), Reconciling Personal Information in the United States and European Union, California Law Review, Volume 102, No. 877, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442

Schwartz Paul & Solove Daniel (2014), Defining 'Personal Data' in the European Union and U.S., Privacy & Security Law Report, No. 13, διαθέσιμο στο https://news.bloomberglaw.com/tech-and-telecom-law/defining-personal-data-in-the-european-union-and-us

Schwartz Paul & Peifer Karl - Nikolaus (2017), Transatlantic Data Privacy Law, Georgetown Law Journal 115, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066971

Schwartz Paul (2019), Global Data Privacy: The EU Way, New York University Law Review 771, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3468554

Sullivan Clare (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, Volume 35, Issue 4, διαθέσιμο στο https://www.sciencedirect.com/science/article/abs/pii/S026736491930038X

Swales Lee (2021), The Protection of Personal Information Act and data de-identification, South African Journal of Science, Volume 117, No. 7-8, διαθέσιμο στο https://sajs.co.za/article/view/10808

Topelson Dalia, Bavitz, Gupta Ritu & Oberman Irina (2013), Privacy and Children's Data - An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act, Berkman Center Research Publication No. 23, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354339

Tovino Stacey (2017), The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons, Scholarly Works 1066, διαθέσιμο στο https://scholars.law.unlv.edu/facpub/1066/

Tzanou Maria (2020), Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights, Data Protection Beyond Borders:Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3710539

United Nations Conference on Trade and Development (2016), Data protection regulations and international data flows: Implications for trade and development, https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

United States Department of Commerce (ND), Privacy, Office of Privacy and Open Government, U.S. Department of Commerce, διαθέσιμο στο https://www.commerce.gov/opog/it-privacy-policy-office-privacy-and-open-government-us-department-commerce#P126_15356

Vogiatzoglou Plixavra & Valcke Peggy (2022), Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law, Research Handbook on EU data protection, Edward Elgar, διαθέσιμο στο https://www.elgaronline.com/edcollchap/edcoll/9781800371675/9781800371675.00010.xml

Vogel David & Kagan Robert (2002), Dynamics of Regulatory Change: How Globalization Affects National Regulatory Policies, διαθέσιμο στο https://escholarship.org/uc/item/4qf1c74d

Vogel David (2012), Politics of precaution: Regulating health, safety, and environmental risks in Europe and the United States, διαθέσιμο στο https://www.researchgate.net/publication/286214512_The_politics_of_precaution_Regulating_health_safety_and_environmental_risks_in_Europe_and_the_United_States

Volini Anthony (2023), The Right to Data Privacy: Revisiting Warren & Brandeis, Northwestern Journal of Technology and Intellectual Property, Volume 21, Issue 1, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4421290

Voss Gregory & Houser Kimberly (2019), Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies, American Business Law Journal 287-344, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3389515

Voss Gregory (2020), Cross – Border Data Flows, the GDPR, and Data Governance, Washington International Law Journal Association 485, διαθέσιμο στο https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7/

Voss Gregory (2021), The CCPA and the GDPR Are Non the Same: Why You Should Understand Both, CPI Antitrust Chronicle, Jan. 2021, Volume 1, No. 1, διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3769825

Waller Spencer, Heidtke Daniel & Stewart Jessica (2021), The Telephone Consumer Protection Act of 1991: Adapting Consumer Protection to Changing Technology, Public Law & Legal Theory Research Paper, No. 2013-016, διαθέσιμο στο https://lawecommons.luc.edu/lclr/vol26/iss3/2/

Wang Flora (2020), Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement, Harvard Journal of Law & Technology Volume 33, Number 2, διαθέσιμο στο https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf

Warren Christopher (1998), In the stream of history: shaping foreign policy for a new era, Stanford University Press

Watts David & Casanovas Pompeu (2017), Privacy and Data Protection in Australia: a Critical overview, Data Privacy Controls and Vocabularies.: A W3C Workshop on Privacy and Linked Data, διαθέσιμο στο https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf

Westin Alan (1968), Privacy And Freedom, Washington and Lee Law Review, Volume 25, Issue 1, https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/

Working Party 29 (2016), Opinion 1/2016 of 13 April 2016 on the EU–U.S. Privacy Shield draft adequacy decision WP 238; Resolution of the Parliament of 6 April 2017 on the adequacy of the protection afforded by the EU–US Privacy Shield, P8_TA(2017)0131, para 17;., διαθέσιμο στο https://ec.europa.eu/newsroom/article29/items/640157/en,

Young Alasdair R. (2003), Political Transfer and "Trading Up"? Transatlantic Trade in Genetically Modified Food and U.S. Politics, Vol. 55, No. 4. World Politics, διαθέσιμο στο https://www.jstor.org/stable/25054235

3. ΝΟΜΟΘΕΣΙΑ

Γενικός Κανονισμός Προστασίας Δεδομένων (2016), Γενικός Κανονισμός Προστασίας Δεδομένων (ΕΕ) 2016/679 (με **ενσωματωμένες** μεταγενέστερες διορθώσεις) 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, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, (1953), διαθέσιμο στο **https://www.echr.coe.int/documents/d/echr/convention_ell**

Οδηγία 95/46/ΕΚ (1995), 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 εδώ https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:31995L0046

Σύμβαση 108 (1981), Σύμβαση 108 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, διαθέσιμο στο https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

Σύμβαση 108+ (2018), Σύμβαση 108 + για την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, διαθέσιμο στο https://search.coe.int/cm#{%22CoEObjectId%22:[%2209000016807c65bf%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

Χάρτης Θεμελιωδών Δικαιωμάτωνν (2000), διαθέσιμο στο https://www.europarl.europa.eu/charter/pdf/text_el.pdf

Συνθήκη της Λισσαβώνας (2007), Συνθήκη της Λισσαβώνας, για την τροποποίηση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης περί ιδρύσεως της Ευρωπαϊκής Κοινότητας (2007/ C 306/01), διαθέσιμο στο https://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0006.01/DOC_19

Act on the Protection of Personal Information (2003), Act No. 57 of 2003, διαθέσιμο στο https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

American Privacy Rights Act (2024), το νομοσχέδιο διαθέσιμο στο https://www.congress.gov/bill/118th-congress/house-bill/8818?q=%7B%22search%22%3A%22american+privacy+rights+act%22%7D&s=1&r=1

California Consumer Privacy Act (2018), Title 1.81.5 added by Stats. 2018, Chapter 55, Section 3, διαθέσιμο στο https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Children's Online Privacy Protection Act (1998), Title 16 Chapter I Subchapter C Part 312, διαθέσιμο στο https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Controlling the Assault of Non-Solicited Pornography and Marketing Act (2003), Title 16 Chapter I Subchapter C Part 316, διαθέσιμο στο https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-316

Foreign Account Tax Compliance Act (2010), διαθέσιμο στο https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca

Fair Credit Reporting Act (1970), 15 U.S.C. § 1681, διαθέσιμο στο https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act

General Personal Data Protection Law (2018), Law 13709/2018, διαθέσιμο στο https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Gramm-Leach-Bliley Act (1999), 15 U.S.C. § 6801 et seq., διαθέσιμο στο https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

Health Insurance Portability and accountability Act (1996), διαθέσιμο στο https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Personal Information Protection and Electronic Documents Act (2000), S.C. 2000, c. 5, διαθέσιμο εδώ https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html

Personal Information Protection Law (2021), διαθέσιμο στο http://www.npc.gov.cn/npc/index.html

Protection of Personal Information Act (2013), Law No. 37067/2014, διαθέσιμο στο https://popia.co.za/

PRIVACY ACT (1974), 5 U.S.C. § 552a, διαθέσιμο στο https://www.justice.gov/opcl/privacy-act-1974

PRIVACY ACT (1988), No. 119, 1988, διαθέσιμο στο https://www.legislation.gov.au/C2004A03712/latest/text

Stop Hacks and Improve Electronic Data Security Act (2019), διαθέσιμο στο https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

Telephone Consumer Protection Act (1991), 47 U.S.C. § 227, διαθέσιμο εδώ https://www.fcc.gov/sites/default/files/tcpa-rules.pdf

4. ΝΟΜΟΛΟΓΙΑ

Δικαστήριο Ευρωπαϊκής Ένωσης (2014), Απόφαση του Δικαστηρίου της 13ης Μαΐου 2014, στην υπόθεση C-131/12, στο πλαίσιο της δίκης Google Spain SL κατά Agencia Española de Protección de Datos (AEPD), διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62012CJ0131,

Δικαστήριο Ευρωπαϊκής Ένωσης (2015), Απόφαση του Δικαστηρίου της 6ης Οκτωβρίου 2015, στην υπόθεση C-362/14, στο πλαίσιο της δίκης Maximillian Schrems κατά Data Protection Commissioner, παρισταμένου του: Digital Rights Ireland Ltd, διαθέσιμο στο https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EL

Δικαστήριο Ευρωπαϊκής Ένωσης (2020), Απόφαση της 16ης Ιουλίου 2020 στην υπόθεση C-311/18, στο πλαίσιο της δίκης Schrems κατά Facebook Ireland, διαθέσιμο στο https://curia.europa.eu/juris/liste.jsf?num=C-311/18

Ευρωπαϊκό Δικαστήριο για τα Δικαιώματα του Ανθρώπου (2024), Συλλογή νομολογίας σε υποθέσεις που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα, διαθέσιμο στο https://www.echr.coe.int/documents/d/echr/FS_Data_ENG

5. ΑΠΟΦΑΣΕΙΣ ΕΥΡΩΠΑΙΚΗΣ ΕΠΙΤΡΟΠΗΣ

Ευρωπαϊκή Επιτροπή (2000), Απόφαση της Επιτροπής, της 26ης Ιουλίου 2000 (2000/520/ΕΚ), 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, https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32000D0520 (τελευταία προσπέλαση: 21 Απριλίου 2024)

Ευρωπαϊκή Επιτροπή (2010), Απόφαση της Επιτροπής της 5ης Φεβρουαρίου 2010 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [κοινοποιηθείσα υπό τον αριθμό Ε(2010) 593], διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32010D0087

Ευρωπαϊκή Επιτροπή (2013), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο όσον αφορά τη λειτουργία του ασφαλούς λιμένα από τη σκοπιά των

πολιτών της Ένωσης και των εταιρειών που είναι εγκατεστημένες στην EE/COM/2013/847 final/, https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52013DC0847 (τελευταία προσπέλαση: 21 Απριλίου 2024)

Ευρωπαϊκή Επιτροπή (2016), Εκτελεστική Απόφαση (ΕΕ) 2016/1250 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%3A32016D1250

Ευρωπαϊκή Επιτροπή (2017), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, «Ανταλλαγή και προστασία των δεδομένων προσωπικού χαρακτήρα σε έναν παγκοσμιοποιημένο κόσμο», 10.1.2017 COM (2017) 7 final, https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A52017DC0007 (τελευταία προσπέλαση: 9 Ιουνίου 2024)

Ευρωπαϊκή Επιτροπή (2023), Εκτελεστική απόφαση (ΕΕ) 2023/1795 της 10ης Ιουλίου 2023 σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επάρκεια του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα βάσει του πλαισίου ΕΕ-ΗΠΑ για την προστασία των δεδομένων, διαθέσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32023D1795

Ευρωπαϊκό Κοινοβούλιο (2023), Ψήφισμα της 11ης Μαΐου 2023 σχετικά με την επάρκεια της προστασίας που παρέχεται από το πλαίσιο προστασίας δεδομένων ΕΕ-ΗΠΑ (2023/2501(RSP)), διαθέσιμο στο https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EL.pdf

6. ΛΟΙΠΕΣ ΠΗΓΕΣ

APEC (ND), Member-Economies, διαθέσιμο στο https://www.apec.org/about-us/about-apec/member-economies (τελευταία προσπέλαση: 17 Απριλίου 2024)

ASEAN (ND), About us, διαθέσιμο στο https://asean.org/about-us/ (τελευταία προσπέλαση: 17 Απριλίου 2024)

Council of Europe (ND), Member States of CoE, διαθέσιμο στο https://www.coe.int/el/web/about-us/our-member-states (τελευταία προσπέλαση: 21 Απριλίου 2024)

CIA WORLD FACTBOOK (2024), Explore All Countries, διαθέσιμο στο https://www.cia.gov/the-world-factbook/countries/ (τελευταία προσπέλαση: 22 Απριλίου 2024)

Data Guidance (ND), US Privacy Laws, διαθέσιμο στο https://www.dataguidance.com/comparisons/usa-privacy-laws (τελευταία προσπέλαση: 21 Μαρτίου 2024)

Data Guidance (ND), USA : American Privacy Rights Act, διαθέσιμο στο https://www.dataguidance.com/opinion/usa-american-privacy-rights-act-qa (τελευταία πρόσβαση 22 Αυγούστου 2024)

Data Guidance (2023), China - Data Protection Overview, Guidance Note , διαθέσιμο στο https://www.dataguidance.com/notes/china-data-protection-overview (τελευταία προσπέλαση: 9 Ιουνίου 2024)

European Parliament (2022), Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739261 (τελευταία προσπέλαση: 22 Απριλίου 2024)

Facebook (2018), Facebook's Commitment to Data Protection and Privacy in Compliance with the GDPR, διαθέσιμο στο https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr (τελευταία προσπέλαση: 22 Απριλίου 2024)

Google (2018), Privacy Policy, διαθέσιμο εδώ https://policies.google.com/privacy/archive/20180525?hl=en-US (τελευταία προσπέλαση: 22 Απριλίου 2024)

Microsoft (2018), Microsoft's commitment to GDPR, privacy and putting customers in control of their own data, διαθέσιμο εδώ https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ (τελευταία προσπέλαση: 22 Απριλίου 2024)

Microsoft (2024), Privacy Statement, https://privacy.microsoft.com/el-GR/privacystatement#maincaliforniaconsumerprivacyactmodule (τελευταία προσπέλαση: 22 Απριλίου 2024)

N.Y. TIMES (ND), Microsoft: There's a Data Crackdown Coming. Why It's Good for Customers and Business, διαθέσιμο εδώ https://www.nytimes.com/paidpost/microsoft/theres-a-data-crackdown-coming.html (τελευταία προσπέλαση: 22 Απριλίου 2024).

OECD (ND), About the Organisation for European Economic Co-operation (OEEC), διαθέσιμο στο https://www.oecd.org/en/about/history/the-organisation-for-european-economic-co-operation-oeec.html (τελευταία προσπέλαση: 21 Απριλίου 2024)