ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021- 2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Ηλιάνας Ι. Παπαντώνη (Α.Μ.: ΜΔΙ2035)

ΚΑΘ' ΟΔΟΝ ΠΡΟΣ ΤΗΝ ΥΙΟΘΕΤΗΣΗ ΤΟΥ ePRIVACY. Η ΠΡΟΣ ΡΥΘΜΙΣΗ ΥΛΗ ΚΑΙ ΤΑ ΔΙΑΚΥΒΕΥΜΑΤΑ ΤΟΥ ΝΕΟΥ ΚΑΝΟΝΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ.

Επιβλέπουσα:

Δρ. Αικατερίνα Παπανικολάου

Πειραιάς, Ιούνιος 2022

Στην καλύτερη οικογένεια
που θα μπορούσα να έχω ζητήσει.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΔΑΕ	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
ΑΠ	Άρειος Πάγος
Αρ.	Άρθρο
Βλ.	Βλέπε
ΓΚΠΔ	Γενικός Κανονισμός Προσωπικών Δεδομένων
ΔΕΕ	Δικαστήριο Ευρωπαϊκής Ένωσης
Εδ.	Εδάφιο
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
Επ.	Επόμενα
ΕΚ	Ευρωπαϊκό Κοινοβούλιο
ΕΟΚΕ	Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΕΣΠΔ	Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων
Κ.ά.	Και άλλα
Κ.λπ.	Και τα λοιπά
Ν.	Νόμος
ΠΔ	Προεδρικό Διάταγμα
Περ.	Περίπτωση
Π.χ.	Παραδείγματος Χάριν
ΠΚ	Ποινικός Κώδικας
Σ.	Σύνταγμα
Σελ.	Σελίδα
ΣτΕ	Συμβούλιο της Επικρατείας
ΦΕΚ	Φύλλο Εφημερίδας της Κυβερνήσεως
ΨΕΑ	Στρατηγική Ενιαία Αγορά
AI	Artificial Intelligence
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite Systems
IoT	Internet Of Things

ΠΡΟΛΟΓΟΣ

Στην παρούσα διπλωματική εργασία, η οποία πραγματοποιείται στο πλαίσιο του μεταπτυχιακού προγράμματος του Πανεπιστημίου Πειραιώς «Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών», θα επιχειρηθεί η ανάλυση του Κανονισμού «*για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες)*», με βάση το τελικό Σχέδιο, το οποίο έγινε δεκτό από το Συμβούλιο της Ευρωπαϊκής Ένωσης στις 10 Φεβρουαρίου 2021, παρά το γεγονός ότι έως σήμερα δεν έχει ψηφιστεί από το Ευρωπαϊκό Κοινοβούλιο, αλλά ούτε υπάρχει κάποια σχετική ενημέρωση για την ακριβή ημερομηνία ψήφισής του.

Αρχικά, στο δεύτερο κεφάλαιο της παρούσας θα αναλυθεί η έννοια της ιδιωτικότητας εν γένει και οι λόγοι που της προσδίδουν εξέχουσα θέση στα προστατευόμενα έννομα αγαθά. Εν συνεχεία και ειδικότερα, θα αναλυθεί η ανάγκη προστασίας του απορρήτου των επικοινωνιών, υπό τον κίνδυνο, μάλιστα, των νέων τεχνολογιών και των νέων μορφών επικοινωνίας και στο τρίτο κεφάλαιο θα αναφερθεί το νομικό πλαίσιο που καλύπτει το απόρρητο έως και σήμερα, τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο.

Το τέταρτο κεφάλαιο θα ασχοληθεί εκτενώς με το νομοθετικό κενό, το οποίο θα καλυφθεί από τον Κανονισμό και με το ίδιο το κείμενο του Κανονισμού, αναπτύσσοντας τις επιμέρους έννοιες που εντοπίζονται σε αυτό και παρουσιάζουν τόσο νομικό όσο και τεχνολογικό ενδιαφέρον, όπως είναι παραδείγματος χάριν τα μεταδεδομένα ή οι πληροφορίες που βρίσκονται στον τερματικό εξοπλισμό του χρήστη.

Στο πέμπτο κεφάλαιο της παρούσας θα γίνει μια επισκόπηση του Κανονισμού αναφορικά με τις ρυθμίσεις τις οποίες θεσπίζει καθώς και των αλλαγών που έχουν επέλθει στο συνολικό του κείμενο από την πρόταση της Ευρωπαϊκής Επιτροπής στις 10.01.2017 έως το σχέδιο της 10ης.02.2021, το οποίο και έγινε δεκτό από το Συμβούλιο της Ευρωπαϊκής Ένωσης.

Θα αναφερθεί, καταληκτικά, η μακρά διαδρομή την οποία έχει ήδη διανύσει ο Κανονισμός έως την ψήφισή του, η οποία εντούτοις δεν φαίνεται ακόμη στον ορίζοντα, γεγονός καθόλου ενθαρρυντικό για το μέλλον της ιδιωτικότητας ιδίως στον τομέα των παραδοσιακών μορφών αλλά και των ριζοσπαστικών μορφών επικοινωνίας. Επίσης, θα αναφερθούν οι πιθανότεροι λόγοι για τους οποίους μέχρι σήμερα δεν έχει περατωθεί η διαδικασία ψήφισης του Κανονισμού, ώστε να πραγματοποιηθεί και η γραφή της παρούσας σε μια άλλη βάση.

Τέλος, θα καταλήξει η παρούσα στα συμπεράσματα της γράφουσας αναφορικά με το κείμενο του Κανονισμού, τις επιφυλάξεις που έχουν διατυπωθεί καθώς και με την κατάσταση που έχει δυσμενώς δημιουργηθεί με την τεράστια καθυστέρηση της διαδικασίας ψήφισης του Κανονισμού.

Ι. ΕΙΣΑΓΩΓΗ

Λίγους μήνες μετά από την ψήφιση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ/ GDPR), η Ευρωπαϊκή Επιτροπή στις 10.01.2017 υπέβαλε Πρόταση Κανονισμού[1] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «*για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες)*», τον λεγόμενο Κανονισμό ePrivacy, ο οποίος θα μελετηθεί με την παρούσα και χάριν ευκολίας θα αναφέρεται ως ο «Κανονισμός».

Η πρόταση αυτή της Επιτροπής έκανε λόγο για τον στόχο της στρατηγικής για την ψηφιακή ενιαία αγορά («στρατηγική ΨΕΑ»), ο οποίος δεν είναι άλλος από την ενίσχυση της εμπιστοσύνης στις ψηφιακές υπηρεσίες και στην ασφάλεια των υπηρεσιών αυτών. Βασικό βήμα προς την κατεύθυνση αυτή υπήρξε η υιοθέτηση του ΓΚΠΔ, ενώ το επόμενο βήμα είναι η αναθεώρηση της οδηγίας 2002/58/ΕΚ «*σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)*», ώστε να προστατεύεται με τον καλύτερο δυνατό τρόπο η ιδιωτική ζωή των χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών και να παρέχονται παράλληλα ισότιμοι όροι ανταγωνισμού σε όλους τους παράγοντες της αγοράς[2]. Η αναθεώρηση αυτή θα επιτευχθεί με την υλοποίηση της συγκεκριμένης πρότασης της Επιτροπής, ήτοι με τη θέση σε εφαρμογή του Κανονισμού ePrivacy, ο οποίος θα συμπληρώσει τον ΓΚΠΔ[3], έχοντας μεταξύ τους σχέση ειδικού προς γενικό.

Ο Ευρωπαϊκός Επόπτης Προστασίας Δεδομένων με τη με αριθμό 06.2017 Γνωμοδότησή του επί της πρότασης της Επιτροπής και του πρώτου Σχεδίου (01.2017) του Κανονισμού[4], πολύ ορθά σημείωσε ότι χωρίς τον Κανονισμό ePrivacy, το νομοθετικό πλαίσιο της Ένωσης όσον αφορά στην ιδιωτικότητα και στην προστασία των δεδομένων θα είναι ελλιπές και ότι ένας

[1] Το κείμενο της πρότασης του Κανονισμού της Επιτροπής στις 10.01.2017, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

[2] Βλ. αναλυτικά την «Αιτιολογική Έκθεση» της από 10.01.2017 Πρότασης της Επιτροπής (σελ. 2).

[3] Παράλληλα ο ΓΚΠΔ ορίζει στο άρθρο 95 με τίτλο «*Σχέση με την οδηγία 2002/58/ΕΚ*» ότι: «*Ο παρών κανονισμός δεν επιβάλλει πρόσθετες υποχρεώσεις σε φυσικά ή νομικά πρόσωπα σε σχέση με την επεξεργασία όσον αφορά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό σε δημόσια δίκτυα επικοινωνίας στην Ένωση σε σχέση με θέματα τα οποία υπόκεινται στις ειδικές υποχρεώσεις με τον ίδιο στόχο που ορίζεται στην οδηγία 2002/58/ΕΚ.*»

[4] Διαθέσιμη ολόκληρη εδώ: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf και συνοπτική του παρουσίαση εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017XX0720(01)&from=EN

Κανονισμός ο οποίος θα προστατεύει την ιδιωτική ζωή των προσώπων με ειδικότερη μνεία στο απόρρητο των επικοινωνιών, αποτελεί απαραίτητο βέλος στη νομοθετική φαρέτρα της Ένωσης. Ο Κανονισμός ePrivacy, επομένως, εξειδικεύοντας τον Γενικό Κανονισμός Προστασίας Δεδομένων και αποτελώντας με τον τρόπο αυτό «lex specialis», θα συμπληρώσει το «παζλ» του κανονιστικού πλαισίου της Ένωσης προς την αποτελεσματικότερη προστασία της ιδιωτικότητας, παρέχοντας πρόσθετες ισχυρές εγγυήσεις αναφορικά με την προστασία του απορρήτου των ηλεκτρονικών επικοινωνιών[5].

Στις 05.07.2017 γνωμοδότησε σχετικά η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή[6], η οποία εξέφρασε μάλλον αποδοκιμαστικά σχόλια επί της πρότασης της Επιτροπής, κάνοντας λόγο για ένα κείμενο το οποίο δύνανται να αντιληφθούν μόνο οι μυημένοι και δεν είναι ευχερές να αντιληφθεί ο απλός πολίτης, φέρνοντάς τον με τον τρόπο αυτό σε αρκετά δυσμενή θέση, αφού καθίσταται σχεδόν ανέφικτο να ασκήσει τα δικαιώματά του, τα οποία πηγάζουν από τον Κανονισμό. Παράλληλα, κάνει ειδική μνεία αναφορικά με τις επιλογές που είχαν διατεθεί στη διάθεση της Επιτροπής για την επίτευξη των στόχων[7], βάσει της εκτίμησης επιπτώσεων[8], η οποία συνόδευε την Πρόταση του Κανονισμού στις 10.01.2017, προχωρώντας σε αιχμηρό σχολιασμό σχετικά με την επιλογή της Επιτροπής να ενισχύσει στο ελάχιστο την προστασία της ιδιωτικής ζωής των πολιτών, η οποία, σύμφωνα με τη γνωμοδότηση, θυσιάστηκε στον βωμό των ειδικότερων συμφερόντων της βιομηχανίας. Ειδικότερα, η Επιτροπή επέλεξε από τις 5 προτεινόμενες επιλογές, την επιλογή με αριθμό 3, ήτοι την «*Μέτρια ενίσχυση της ιδιωτική ζωής/ του απορρήτου και εναρμόνιση*», επιλογή για την οποία βρέθηκε στο στόχαστρο της ΕΟΚΕ αφού, όπως χαρακτηριστικά αναφέρει, η Επιτροπή δεν αποσαφήνισε τον λόγο για τον οποίο επιλέχθηκε η επιλογή της μέτριας ενίσχυσης και τον λόγο για τον οποίο η επιλογή μιας «μεγαλύτερης» ενίσχυσης της ιδιωτικής ζωής θα έβλαπτε τυχόν τα συμφέροντα της

[5] Βλ. Δήλωση 03.2021 σχετικά με τον Κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ), διαθέσιμη εδώ: https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_el.pdf

[6] Η Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής επί της πρότασης της Επιτροπής, την οποία υπογράφει ο Πρόεδρός της, κ. Γιώργος Ντάσης, διαθέσιμη εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017AE0655&from=EN

[7] Ως ειδικοί στόχοι της αναθεώρησης ορίστηκαν, βάσει της ίδιας εκτίμησης επιπτώσεων, οι εξής: 1. Η διασφάλιση της αποτελεσματικής τήρησης του απορρήτου των ηλεκτρονικών επικοινωνιών, 2. Η διασφάλιση της αποτελεσματικής προστασίας έναντι των μη ζητηθεισών εμπορικών επικοινωνιών και 3. Η προώθηση της εναρμόνισης και απλούστευση/ επικαιροποίηση του νομικού πλαισίου.

[8] Ολόκληρο το κείμενο της Περίληψης της Εκτίμησης Επιπτώσεων, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2017%3A0004%3AFIN

βιομηχανίας. Η ΕΟΚΕ, τέλος, πέραν της έντονης κριτικής προχώρησε και σε συνολικά 14 συστάσεις προς την Επιτροπή με την ελπίδα να εξασφαλιστεί η καλύτερη δυνατή προστασία των πολιτών, κατά προτεραιότητα.

Εντέλει, το σχέδιο του Κανονισμού έγινε δεκτό από το Συμβούλιο της Ευρωπαϊκής Ένωσης στις 10.02.2021[9], το οποίο και θα αναλυθεί με την παρούσα, ως το τελευταίο σχέδιό του. Ως εκ τούτου, κατωτέρω θα αναλυθούν οι επιμέρους έννοιες που εντοπίζονται σε αυτό, οι ρυθμίσεις του, θα συγκριθούν τα κείμενα της αρχικής πρότασης της Επιτροπής (01.2017) με το σχέδιο που εντέλει έγινε δεκτό (02.2021), ώστε να μπορέσουμε να προχωρήσουμε σε κάποια ασφαλή συμπεράσματα αναφορικά με τις αλλαγές που θα επιφέρει ο Κανονισμός ως προς την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες φυσικών και νομικών προσώπων, πάντοτε με γνώμονα τον ίδιο τον άνθρωπο ή εάν τελικά οι θεσμοί θα «υποκύψουν» στις πιέσεις των τεχνολογικών κολοσσών και επομένως βρισκόμεθα στη δίνη ενός φαύλου κύκλου που εντέλει δεν θα καταλήξει πουθενά.

[9] Το από 10.02.2021 σχέδιο του Κανονισμού, που έγινε δεκτό από το Ευρωπαϊκό Συμβούλιο, διαθέσιμο εδώ: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_6087_2021_INIT

ΙΙ. Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

ΙΙ.1. Το δικαίωμα στην ιδιωτικότητα

Η προστασία του ιδιωτικού βίου του ατόμου έχει κατοχυρωθεί από διεθνείς συμβάσεις και σε εθνικό επίπεδο από τον θεμελιώδη νόμο, το Σύνταγμα. Ως έννοια, η «ιδιωτικότητα» περιγράφεται εντελώς συνοπτικά αλλά και απολύτως εύστοχα με τη φράση «*the right to be left alone*»[10] (το δικαίωμα του να μένει κανείς μόνος του), ήτοι το δικαίωμα να προστατεύει το άτομο τις διάφορες εκφάνσεις της ζωής του από τα αδιάκριτα βλέμματα τρίτων[11].

Η αξία της ιδιωτικότητας συνοψίζεται στη δυνατότητά της να παρέχει στο πρόσωπο το δικαίωμα να απαντά με τρόπο αρνητικό και αμυντικό προς κάθε εισβολή ή παρέμβαση που δέχεται στον προσωπικό του χώρο καθώς και στην προστασία από οιαδήποτε καταπιεστική, χειραγωγική, ελεγκτική ή πατερναλιστική συμπεριφορά, η οποία έχει ως αποτέλεσμα τον περιορισμό της ελευθερίας του ατόμου, τον περιορισμό της απρόσκοπτης ανάπτυξης της προσωπικότητάς του και εν γένει όλων των επιλογών, μέσα από τις οποίες εντέλει αυτοπροσδιορίζεται[12]. Εφόσον υφίσταται η αρνητική και αμυντική προστασία του προσώπου, αυτό δύναται να χτίσει τη ζωή του ελεύθερα και όπως την επιθυμεί, να αναπτύξει την προσωπικότητά του κατά το δοκούν, να επικοινωνεί και να εκφράζεται χωρίς φόβο κ.λπ.

Παρά το γεγονός ότι με μια επιφανειακή ματιά η έννοια της ιδιωτικότητας μπορεί να ταυτίζεται με την έννοια των προσωπικών δεδομένων, η ιδιωτικότητα εμφανίζεται ως νοηματικά ευρύτερη αυτής των προσωπικών δεδομένων. Έτσι, θα πρέπει, αρχικά, να διαμορφωθεί από τον νομοθέτη ένα προστατευτικό νομοθετικό πλαίσιο εντός του οποίου θα χαίρει της προστασίας που του αρμόζει ο ιδιωτικός βίος του ατόμου και σε συνέχεια αυτού θα καθίσταται η συλλογή και επεξεργασία των προσωπικών δεδομένων σύννομη και θεμιτή[13]. Πρόκειται, εντούτοις, για μια εγγενή σχέση στον βαθμό που το δικαίωμα του προσώπου στην προστασία των προσωπικών δεδομένων εξελίσσεται με σκοπό να αντιμετωπίσει τις

[10] Πρόκειται για φράση, η οποία αποτυπώθηκε στο άρθρο των Samuel Warren και Louis Brandeis, «*The Right to Privacy*», Harvard Law Review, Vol. 4, No 5 (Dec. 15, 1890), pp. 193- 220.
[11] Λ. Κανέλλος, «*The GDPR Handbook*», Νομική Βιβλιοθήκη, 2020, σελ. 88.
[12] Χ. Ακριβοπούλου, «*Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή*», Νομική Βιβλιοθήκη, ΘΠΔΔ, 7/2011, σελ. 680.
[13] Γ. Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018, σελ. 67.

καινοφανείς διακινδυνεύσεις της προστασίας της ιδιωτικής ζωής, οι οποίες γεννώνται από τη διαρκώς αναπτυσσόμενη Κοινωνία της Πληροφορίας[14].

Η διαρκής ανάπτυξη της τεχνολογίας σε συνδυασμό με την απεριόριστη πλέον δυνατότητα να αντλεί κανείς σημαντικές πληροφορίες από την πρόσβαση και επεξεργασία των δεδομένων που προκύπτει από τις τηλεφωνικές επικοινωνίες, θέτει, αν μη τι άλλο, σε σημαντικό κίνδυνο την ιδιωτικότητα του ατόμου, καθιστώντας με τον τρόπο αυτό επιτακτικότερη παρά ποτέ την προστασία της τελευταίας με την παράλληλη εξέλιξη του νομοθετικού πλαισίου που την προστατεύει[15].

ΙΙ.2. Η ανάγκη προστασίας του απορρήτου των επικοινωνιών και της ιδιωτικότητας κατά τη χρήση νέων τεχνολογιών μέσω ενός ενιαίου κειμένου

Η επικοινωνία αποτελεί έναν στοιχείο μείζονος σημασίας για την ίδια τη ζωή του ανθρώπου, η οποία τον βοηθά μέσω του γραπτού ή του προφορικού λόγου να έρχεται σε επαφή με άλλους ανθρώπους, να ξετυλίγει τις σκέψεις, τις ιδέες και τα συναισθήματά του και εν γένει την προσωπικότητά του.

Από το περιεχόμενο μιας επικοινωνίας είναι κανείς σε θέση να αντλήσει πολλές πληροφορίες και γεγονότα που αφορούν τις ιδιαίτερες πτυχές της προσωπικότητας των επικοινωνούντων, τις σεξουαλικές τους προτιμήσεις, το ιατρικό τους ιστορικό, την πολιτική τους θέση και άλλα στοιχεία του χαρακτήρα ενός ανθρώπου, τα οποία πιθανότατα να μην επιθυμεί να γνωρίζουν τρίτοι.

Το ίδιο ισχύει, κατά τον Κανονισμό[16] και για τα μεταδεδομένα της επικοινωνίας, τα οποία μπορούν να αποκαλύψουν στοιχεία όπως τους καλούντες αριθμούς του χρήστη, τη γεωγραφική θέση του καλούντος, την ώρα και την ημερομηνία κ.ά., στοιχεία τα οποία οδηγούν αν μη τι άλλο σε ακριβή συμπεράσματα για την προσωπική ζωή ενός προσώπου, την οποία και οφείλει ο νόμος να προστατεύσει.

---

[14] Δεν εντοπίζεται ένας γενικά αποδεκτός ορισμός για την έννοια της «Κοινωνίας της Πληροφορίας». Πρώτη φορά εμφανίστηκε το 1998 ως: «*υπηρεσία της κοινωνίας των πληροφοριών είναι κάθε υπηρεσία που συνήθως παρέχεται έναντι αμοιβής, με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν προσωπικής επιλογής ενός αποδέκτη υπηρεσιών*». Βλ. αναλυτικότερα περί του όρου: Γ. Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018, σελ. 34 επ.

[15] Γρ. Τσόλιας, «*Τα τηλεπικοινωνιακά δεδομένα υπό το πρίσμα του απορρήτου: προβληματισμοί εν όψει της ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ*», ΔiΜΕΕ, 2004, σελ. 360 επ.

[16] Βλ. αιτιολογική σκέψη 2 του Σχεδίου 02.2021 του Κανονισμού.

Ειδικής προστασίας πρέπει να χαίρουν, σύμφωνα με τον Κανονισμό, και οι επιφυείς υπηρεσίες[17] (Over the Top communication services), οι υπηρεσίες machine to machine[18], οι επικοινωνίες που πραγματοποιούνται μεταξύ των «έξυπνων συσκευών» (Internet of Things)[19], οι πληροφορίες που συλλέγονται από τις τελευταίες και οι επικοινωνίες μέσω ασύρματων δικτύων.

Όσον αφορά στα νομικά πρόσωπα, τα δεδομένα μια επικοινωνίας δύνανται να αποκαλύψουν στοιχεία όπως είναι η οικονομική κατάσταση μιας εταιρείας για παράδειγμα, πιθανές νομικές εκκρεμότητες που αντιμετωπίζει κ.ά., τα οποία μπορούν να κλονίσουν την αξιοπιστία της στην αγορά και να της προκαλέσουν σοβαρό πλήγμα.

Για όλους τους ανωτέρω λόγους είναι υψίστης σημασίας η προστασία του περιεχομένου και των μεταδεδομένων της επικοινωνίας των νέων τεχνολογιών, αναφορικά τόσο με τα φυσικά όσο και με τα νομικά πρόσωπα για τη σύγχρονη κοινωνία αλλά και για την οικονομία[20] μέσω ενός κειμένου το οποίο θα τυγχάνει εφαρμογής ενιαία σε όλα τα κράτη- μέλη.

---

[17] Ως επιφυής (Over The Top) υπηρεσία ορίζεται: «*το περιεχόμενο, η υπηρεσία ή η εφαρμογή, η οποία προσφέρεται στον τελικό χρήστη μέσω του δημόσιου Διαδικτύου*». Συνεπώς οι Over the Top Communication Services είναι οι υπηρεσίες επικοινωνιών που παρέχονται μέσω διαδικτύου, όπως είναι οι δημοφιλείς πλέον εφαρμογές, Messenger, Viber κ.ά. Βλ. ειδικότερα Body of European Regulator for Electronic Communications (BEREC) Report on OTT Services, διαθέσιμο εδώ: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services

[18] Machine to machine (M2M) είναι ο όρος που χρησιμοποιείται για να περιγράψει την τεχνολογία, η οποία επιτρέπει στις έξυπνες συσκευές να ανταλλάσσουν απευθείας δεδομένα μεταξύ τους, χωρίς ανθρώπινη παρέμβαση.

[19] Το Διαδίκτυο των Πραγμάτων, αγγλιστί το Internet of Things, αποτελεί ένα δίκτυο παγκόσμιας εμβέλειας, το οποίο διασυνδέει φυσικά και εικονικά αντικείμενα, όπως, ενδεικτικά, οχήματα, συσκευές, ακόμη και ολόκληρες κατοικίες. Προς τον σκοπό αυτό χρησιμοποιούνται τεχνολογίες ανάκτησης δεδομένων και δικτύων επικοινωνίας. Με την αλληλεπίδραση αυτή, στοχεύουν στην κατά το δυνατόν εξυπνότερη και αποδοτικότερη λειτουργία τους. Βλ. αναλυτικότερα: Α. Κουσουνή- Πανταζοπούλου, «*Cloud Computing & Νομικά ζητήματα*», Νομική Βιβλιοθήκη, 2022, σελ. 28 επ.

[20] Βλ. Γνωμοδότηση με αριθμό 06/2017 του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων επί του από 01/2017 Σχεδίου του Κανονισμού, σελ. 7, διαθέσιμη εδώ: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

ΙΙΙ. ΤΟ ΚΑΝΟΝΙΣΤΙΚΟ ΠΛΑΙΣΙΟ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΙΙΙ.1. Το Ευρωπαϊκό κανονιστικό πλαίσιο

ΙΙΙ.1.1. Τα θεμελιώδη Ευρωπαϊκά κείμενα

Η Ευρωπαϊκή νομοθεσία ανέκαθεν έκανε βήματα προς την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων εν γένει και την προστασία των επικοινωνιών των πολιτών των κρατών- μελών της, γεγονός που εμφαίνεται ξεκάθαρα τόσο από τα βασικά της κείμενα προς την προάσπιση των δικαιωμάτων των πολιτών των κρατών- μελών της, όπως είναι η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ)[21] και ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης [22], τα κείμενα των Οδηγιών Data Protection[23], ePrivacy[24] και Cookies[25] έως και τον ΓΚΠΔ και την επερχόμενη ψήφιση του υπό μελέτη Κανονισμού.

Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου, με το άρθρο 8, κατοχύρωσε το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, ενώ προς αυτή την κατεύθυνση κινήθηκε και ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, με το άρθρο 7, επίσης, για τον σεβασμό της ιδιωτικής και οικογενειακής ζωής και με το άρθρο 8 για την προστασία των δεδομένων προσωπικού χαρακτήρα.

ΙΙΙ.1.2. Η οδηγία 95/46/ΕΚ και ο ΓΚΠΔ

---

[21] Η Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, γνωστή πλέον ως Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), υιοθετήθηκε από το Συμβούλιο της Ευρώπης κατά το έτος 1950 και περιέχει συνολικά δεκαέξι πρωτόκολλα. Αποτελεί έως και σήμερα τη μόνη διεθνή συμφωνία προάσπισης και προστασίας των ανθρώπινων δικαιωμάτων. Βλ. ειδικότερα: https://www.echr.coe.int/documents/convention_ell.pdf

[22] Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης υιοθετήθηκε με σκοπό να ενισχυθεί η προστασία των θεμελιωδών δικαιωμάτων πάντοτε σε συνάρτηση με τις μεταβολές που λαμβάνουν χώρα στο κοινωνικό περιβάλλον και με τις ραγδαίες τεχνολογικές εξελίξεις. Στο πλαίσιο αυτό η Ένωση αναγνώρισε τα δικαιώματα, τις ελευθερίες και τις αρχές που αναλυτικά αναφέρονται σε αυτόν σε συνολικά 54 άρθρα. Βλ. ειδικότερα το κείμενο του Χάρτη, διαθέσιμο ηλεκτρονικά εδώ: https://www.europarl.europa.eu/charter/pdf/text_el.pdf

[23] Οδηγία 95/46/ΕΚ, διαθέσιμη ηλεκτρονικά εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL

[24] Οδηγία 2002/58/ΕΚ, διαθέσιμη ηλεκτρονικά εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058

[25] Οδηγία 2009/136/ΕΚ, διαθέσιμη ηλεκτρονικά εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0136&from=EL

Κατά το έτος 1995, υιοθετήθηκε η Οδηγία 95/46/ΕΚ, η οποία αφορούσε στην προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και στην ελεύθερη κυκλοφορία αυτών, η οποία οδηγία καταργήθηκε από τις 25.05.2018, δυνάμει του με αριθμό 94 άρθρου του ΓΚΠΔ. Ο τελευταίος κανονισμός ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο τον Απρίλιο του 2016, με άμεση ισχύ σε όλα τα κράτη- μέλη, καθιστώντας με τον τρόπο αυτό ανίσχυρη οποιαδήποτε αντίθετη νομοθεσία που τυχόν υφίστατο σε αυτά. Στην ελληνική έννομη τάξη ο ΓΚΠΔ ενσωματώθηκε, ακολουθώντας τη διαδικασία του κατεπείγοντος, με τον Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019) [26]. Με τον τελευταίο νόμο ενσωματώθηκε στην ελληνική έννομη τάξη και η οδηγία 2016/680[27], η οποία εφαρμόζεται όσον αφορά στην επεξεργασία προσωπικών δεδομένων των υποκειμένων κατά τη διαδικασία της δίωξης εγκλημάτων από τις διωκτικές Αρχές, ήτοι την Αστυνομία, το Λιμενικό Σώμα, τη Γενική Διεύθυνση Οικονομικού Εγκλήματος κ.λπ.

ΙΙΙ.1.3. Η οδηγία 2002/58/ΕΚ

Ειδικότερα, ως προς την προστασία των επικοινωνιών των πολιτών των κρατών- μελών της Ένωσης, έχει υιοθετηθεί η Οδηγία 2002/58/ΕΚ «*σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)*», γνωστή με την ονομασία «ePrivacy Directive» (Οδηγία ePrivacy), η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 3471/2006. Η εν λόγω οδηγία ήταν αυτή που έθεσε ουσιαστικά τα θεμέλια για την ικανοποιητική προστασία των δεδομένων στο πεδίο των επικοινωνιών[28] και αποτέλεσε lex specialis ήδη η ίδια σε αυτόν τον τομέα[29]. Η οδηγία καλύπτει τις επικοινωνίες που λαμβάνουν χώρα τόσο μέσω σταθερής όσο και κινητής τηλεφωνίας αλλά και μέσω διαδικτύου. Μάλιστα ο ΓΚΠΔ, στο άρθρο 95 όρισε ρητά ότι ο ίδιος κανονισμός «*δεν επιβάλλει πρόσθετες*

[26] Ο ελληνικός νόμος τιτλοφορήθηκε ως εξής: «*Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, προσαρμογή της ελληνικής νομοθεσίας για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαικού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαικού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016*».

[27] Γνωστή και ως «Αστυνομική Οδηγία» (Police Directive). Έως την υιοθέτηση της Οδηγίας αυτής, οι διωκτικές Αρχές εξαιρούντο της εφαρμογής των κανόνων περί προστασίας δεδομένων προσωπικού χαρακτήρα.

[28] Γ. Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018, σελ. 80.

[29] Β. Μπαντή- Μαρκούτη, Αν. Ματσούκα, Μ. Ηλιοπούλου, Τζ. Κιούση «Μεταδεδομένα και ηλεκτρονικές επικοινωνίας: Η κατάργηση της Οδηγίας 2006/24/ΕΚ και η USA Freedom Act 2015», ΔiΜΕΕ, Νομική Βιβλιοθήκη, 3/2015, σελ. 336.

υποχρεώσεις σε φυσικά ή νομικά πρόσωπα σε σχέση με την επεξεργασία όσον αφορά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό σε δημόσια δίκτυα επικοινωνίας στην Ένωση σε σχέση με θέματα τα οποία υπόκεινται στις ειδικές υποχρεώσεις με τον ίδιο στόχο που ορίζεται στην οδηγία 2002/58/ΕΚ».

Ωστόσο, η ραγδαία τεχνολογική εξέλιξη στις ηλεκτρονικές επικοινωνίες, κυρίως με τη χρήση των νέων μορφών επικοινωνίας (π.χ. μέσω messenger, viber κ.λπ.), με τη διασύνδεση μηχανών και υπολογιστικών συστημάτων για την επίτευξη μίας επικοινωνίας, με την διεύρυνση του διαδικτύου των πραγμάτων (IoT) και με την ανάπτυξη της τεχνητής νοημοσύνης (AI)[30], απαιτεί τον εκσυγχρονισμό και τη διεύρυνση του πεδίου που καλύπτει μέχρι σήμερα η οδηγία αλλά και την «αυστηροποίηση» των κανόνων μέσω ενός πιο δεσμευτικού και ενιαίου πλαισίου.

ΙΙΙ.1.4. Η οδηγία 2006/24/ΕΚ

Ιδιαίτερη μνεία πρέπει να γίνει για την οδηγία 2006/24/ΕΚ, γνωστή και ως «Data Retention Directive», η οποία αφορά στη διατήρηση των δεδομένων[31], η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον νόμο 3917/2011, και αποτέλεσε, το δίχως άλλο, μια διφορούμενη οδηγία. Η συγκεκριμένη οδηγία εισήγαγε την υποχρέωση αποθήκευσης για μακρό χρόνο ορισμένων εξωτερικών στοιχείων επικοινωνίας[32] των χρηστών/ συνδρομητών από τους παρόχους των υπηρεσιών, με σκοπό να «*καθίστανται διαθέσιμα για σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων, όπως αυτά ορίζονται βάσει του εθνικού δικαίου των κρατών μελών*»[33]. Πολλώ δε μάλλον, προχώρησε στη ρητή κατάργηση

---

[30] Γρ. Τσόλιας, «*Εξελίξεις στον τομέα της επιτήρησης των ηλεκτρονικών επικοινωνιών: από την Ασφάλεια στην Ελευθερία και τη διεύρυνση της προστατευόμενης επικοινωνίας*», Ποινική Δικαιοσύνη, Νομική Βιβλιοθήκη, Τευχ. 8- 9, Αύγουστος- Σεπτέμβριος, 2017, σελ. 794.

[31] Οδηγία 2006/24/ΕΚ «*για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ*», διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32006L0024&from=GA

[32] Η Οδηγία περιοριζόταν αποκλειστικά στα δεδομένα κίνησης και θέσης και τα λοιπά δεδομένα τα οποία είναι απαραίτητα για την αναγνώριση του χρήστη/ συνδρομητή (βλ. αρ. 1 παρ. 2 της οδηγίας, διαθέσιμη ηλεκτρονικά ως ανωτέρω).

[33] Βλ. άρθρο 1 παρ. 1 της Οδηγίας 2006/24/ΕΚ, διαθέσιμη ηλεκτρονικά ως ανωτέρω.

της σημαντικότατης αρχής της αναλογικότητας[34], η οποία κατοχυρωνόταν με την οδηγία 2002/58/ΕΚ[35].

Οι αντιδράσεις από την ψήφιση της οδηγίας από τα κράτη- μέλη ήσαν πολλές και ποικίλες. Οι αρμόδιες ευρωπαϊκές ανεξάρτητες Αρχές την αποδοκίμασαν έντονα, ενώ πολλά κράτη- μέλη ανέβαλαν ακόμη και την ενσωμάτωση της νέας ρύθμισης στην εσωτερική τους νομοθεσία[36]. Η οδηγία αυτή εντέλει κηρύχθηκε ανίσχυρη από το ΔΕΕ με την απόφαση του Digital Rights Ireland Ltd.[37] (συνεκδικαζόμενες υποθέσεις C- 293/2012 και C- 594/2012), το οποίο κλήθηκε να ελέγξει το νομικό πλαίσιο το οποίο οδηγεί στη διατήρηση των εξωτερικών στοιχείων της επικοινωνίας των χρηστών/ συνδρομητών. Το ΔΕΕ στο ερώτημα «ελευθερία ή ασφάλεια» απήντησε ευτυχώς υπέρ της ελευθερίας[38], κρίνοντας ότι η προληπτική διατήρηση από την πλευρά των παρόχων των εξωτερικών στοιχείων της επικοινωνίας των χρηστών/ συνδρομητών, ακόμη και για την εξακρίβωση σημαντικότατης βαρύτητας εγκλημάτων, όπως είναι η τρομοκρατία, αποτελεί πολύ σοβαρή επέμβαση στην άσκηση των θεμελιωδών δικαιωμάτων του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα των ατόμων, με αποτέλεσμα, μάλιστα, να έχουν την αίσθηση της διαρκούς παρακολούθησης[39].

---

[34] Β. Μπαντή- Μαρκούτη, Αν. Ματσούκα, Μ. Ηλιοπούλου, Τζ. Κιούση «Μεταδεδομένα και ηλεκτρονικές επικοινωνίας: Η κατάργηση της Οδηγίας 2006/24 και η USA Freedom Act 2015», ΔiΜΕΕ, Νομική Βιβλιοθήκη, 3/2015, σελ. 338.

[35] Η οδηγία 2002/58/ΕΚ στο άρθρο 15 παρ. 1 ορίζει ρητά ότι: «*Τα κράτη μέλη δύνανται να λαμβάνουν νομοθετικά μέτρα για να περιορίζουν τα δικαιώματα του υποκειμένου, εφόσον ο περιορισμός αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη της εθνικής ασφάλειας, της δημόσιας ασφάλειας κ.λπ.*». Εντούτοις, η οδηγία 2006/24/ΕΚ στο άρθρο 11 προσέθεσε άρθρο 15 παρ. 1^{α} της οδηγίας 2002/58/ΕΚ το εξής: «*η παράγραφος 1 δεν ισχύει για δεδομένα των οποίων τη διατήρηση προβλέπει ρητά η οδηγία 2006/24/ΕΚ, για τη διατήρηση των δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών, όσον αφορά στους σκοπούς του άρθρου 1 παρ. 1 της εν λόγω οδηγίας*».

[36] Κ. Αρκουλή, «*Προστασία Προσωπικών Δεδομένων στις Ηλεκτρονικές Επικοινωνίες*», Νομική Βιβλιοθήκη, 2010, σελ. 38.

[37] Digital Rights Ireland Ltd. κατά Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform και λοιπών. Διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0293&from=el

[38] Γρ. Τσόλιας, «*Εξελίξεις στον τομέα της επιτήρησης των ηλεκτρονικών επικοινωνιών: από την Ασφάλεια στην Ελευθερία και τη διεύρυνση της προστατευόμενης επικοινωνίας*», Ποινική Δικαιοσύνη, Νομική Βιβλιοθήκη, Τευχ. 8- 9, Αύγουστος- Σεπτέμβριος, 2017, σελ. 790

[39] Το ΔΕΕ δεν έχει μέχρι σήμερα παρεκκλίνει από την άποψη αυτή. Μάλιστα στις 05.04.2022 εξέδωσε απόφαση επί της υπόθεσης με αριθμό C-140/20 (https://curia.europa.eu/juris/document/document.jsf;jsessionid=DBB9D8ADC8D3EAAD57BFEE382A5B783D?text=&docid=257242&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=5042309), δυνάμει της οποίας επιβεβαίωσε την προηγούμενη νομολογία του και έκρινε ότι η καταπολέμηση της

Με την ακύρωση της οδηγίας 2006/24/ΕΚ από το ΔΕΕ[40] επιστρέψαμε στο προηγούμενο νομικό καθεστώς, ήτοι στις δυνατότητες που παρείχε στα κράτη- μέλη το άρθρο 15 § 1 της οδηγίας 2002/58/ΕΚ[41]. Αντίστοιχα, ο υπό εξέταση Κανονισμός, η ψήφιση του οποίου θα καταργήσει την τελευταία οδηγία, περιέχει αντίστοιχου περιεχομένου πρόβλεψη με το άρθρο 11 § 1[42].

ΙΙΙ.1.5. Η οδηγία 2009/136/ΕΚ

Την 25η Νοεμβρίου 2009 το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο εξέδωσαν τον κανονισμό με αριθμό 1211/2009/ΕΚ[43], την οδηγία με αριθμό 2009/136/ΕΚ[44] και την οδηγία με αριθμό 2009/140/ΕΚ[45]. Γνωστότερη εξ αυτών, βέβαια, η οδηγία με αριθμό 2009/136/ΕΚ, γνωστή ως «Cookies Directive», η οποία τροποποίησε αρκετά άρθρα της οδηγίας 2002/22/ΕΚ και της 2002/58/ΕΚ. Με την 66η αιτιολογική σκέψη της εισήγαγε την υποχρέωση παροχής σαφούς και κατανοητής πληροφόρησης στους χρήστες αλλά και λήψης ρητής συγκατάθεσης από τους τελευταίους, όταν τρίτοι σκοπεύουν να αποθηκεύσουν πληροφορίες σχετικά με υλικό που χρησιμοποιούν οι χρήστες ή να αποκτήσουν πρόσβαση σε ήδη αποθηκευμένες πληροφορίες (όπως είναι τα cookies)[46]. Η οδηγία 2009/136/ΕΚ εάν και δεν επέφερε αλλαγές στην ουσία των

σοβαρής εγκληματικότητας, εάν και προφανώς είναι μεγάλης σημασίας, δεν είναι δυνατό να προβληθεί ως μοναδικός λόγος ώστε γενικώς και αδιακρίτως να διατηρούνται δεδομένα κίνησης και θέσης, όπως καθιέρωσε η Οδηγία 2006/24/ΕΚ.

[40] Παρά το γεγονός ότι η οδηγία 2006/24/ΕΚ κηρύχθηκε ανίσχυρη από το ΔΕΕ, ο ελληνικός νόμος 3917/2011 δεν έχει έως και σήμερα καταργηθεί, βλ. ειδικότερα: Γεώργιος Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018, σελ. 81.

[41] Γρ. Τσόλιας, «*Σημείωμα στην συνεκδ. Υποθ. ΔΕΕ C-203/15 και C-689/15, απόφ. της 21.12.2016- Υποχρεωτική διατήρηση δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών*», ΔΙΜΕΕ, 1/2017, σελ. 181.

[42] Βλ. συνδυαστικά και Αιτιολογική Σκέψη 26 του Σχεδίου 02/2021.

[43] Κανονισμός 1211/2009/ΕΚ «*για την ίδρυση του Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC) και της Υπηρεσίες*», διαθέσιμος ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009R1211&from=EL.

[44] Οδηγία 2009/136/ΕΚ «*για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθμ. 2006/2006 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών*», διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0136&from=EL

[45] Οδηγία 2009/140/ΕΚ «*για την τροποποίηση των οδηγιών 2002/21/ΕΚ σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, 2002/19/ΕΚ σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες καθώς και με τη διασύνδεση τους, και 2002/20/ΕΚ για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών*», διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0140&from=EL.

[46] Βλ. την αιτιολογική σκέψη 66 της οδηγίας 2009/136/ΕΚ.

διατάξεων της οδηγίας 2002/58/ΕΚ, αυτές είναι άξιες προσοχής αφού καταδεικνύουν τη σημασία της δημιουργίας των ασφαλέστερων υποδομών ηλεκτρονικών επικοινωνιών για την καλύτερη λειτουργία των λοιπών διατάξεων που αφορούν στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής[47].

III.1.6. Λοιπές οδηγίες και κανονισμοί

Εκδόθηκε, ακόμη, ο με αριθμό 611/2013/ΕΕ[48] κανονισμός της Επιτροπής, οποίος τυγχάνει εφαρμογής κατά την κοινοποίηση των παραβιάσεων προσωπικών δεδομένων από τους παρόχους προς την αρμόδια εθνική Αρχή ή/ και στον συνδρομητή και η οδηγία με αριθμό 2016/1148/ΕΕ [49] του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, δυνάμει της οποίας θεσπίστηκαν μέτρα με σκοπό την επίτευξη υψηλού κοινού επιπέδου ασφαλείας των συστημάτων δικτύου και πληροφοριών εντός της Ευρωπαϊκής Ένωσης, ώστε να λειτουργεί όσο το δυνατόν καλύτερα η εσωτερική αγορά.

Στις 17 Δεκεμβρίου 2018, εξεδόθη η οδηγία 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Δεκεμβρίου 2018 «*για τη Θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών*», δυνάμει της οποίας τροποποιήθηκαν τέσσερις προϋφιστάμενες οδηγίες και ενσωματώθηκαν σε ενιαίο νομικό κείμενο. Η οδηγία αυτή, μεταφέρθηκε στην ελληνική έννομη τάξη με τον Ν. 4727/2020 «*Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2019/1024)- Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις*»[50].

III.2. Το απόρρητο των επικοινωνιών στην ελληνική έννομη τάξη

---

[47] Π. Κίτσος, Π. Παππά «*Ενίσχυση της πληροφόρησης και της διαφάνειας στις υπηρεσίες ηλεκτρονικών επικοινωνιών, υπό το πρίσμα της Οδηγίας 2009/136/ΕΚ*», ΔΙΤΕ, 2/2010.

[48] Ο Κανονισμός 611/2013/ΕΕ «*σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*» τέθηκε σε ισχύ για όλα τα κράτη-μέλη από την 25η.08.2013 (βλ. http://www.adae.gr/fileadmin/docs/pepragmena/2013/files/assets/basic-html/page50.html), διαθέσιμος ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013R0611&from=LV

[49] Η Οδηγία 2016/1148/ΕΕ «*σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση*», ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 4577/2018, διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=EL

[50] Σύμφωνα με την αιτιολογική έκθεση του Ν. 4727/2020 (1η Παράγραφος- ΓΕΝΙΚΑ): «*Ο νέος νόμος έχει στόχο τη σύνταξη ενός μοναδικού ενιαίου νομοθετικού κειμένου με αντικείμενο τη ρύθμιση θεμάτων ψηφιακής διακυβέρνησης στον δημόσιο τομέα*».

III.2.1. Η συνταγματική κατοχύρωση

Το δικαίωμα προστασίας του απορρήτου των επιστολών εμφανίσθηκε για πρώτη φορά στην ελληνική έννομη τάξη με το άρθρο 14[51] του Συντάγματος του 1844[52]. Στο ισχύον Σύνταγμα το εν λόγω δικαίωμα χαίρει προστασίας βάσει του άρθρου 19[53], η πανηγυρική διατύπωση του οποίου, ήτοι η φράση «*απόλυτα απαραβίαστο*», προσδίδει στη διάταξη το ειδικό και συμβολικό βάρος που ο νομοθέτης του 1975 θέλησε να προσδώσει στο εν λόγω δικαίωμα[54]. Με τον τρόπο αυτό ο συνταγματικός νομοθέτης θέλησε να προστατεύσει το απόρρητο των επιστολών και των επικοινωνιών με έναν, αν μη τι άλλο, απόλυτο τρόπο, προβλέποντας, ωστόσο, δύο εξαιρέσεις στον κανόνα αυτό, οι οποίες θα αναλυθούν κατωτέρω (βλ. κατωτέρω, παράγραφο ΙΙΙ.3.). Με την απλή ανάγνωση του άρθρου, γίνεται αντιληπτό, ότι αποτελείται από δύο συνιστώσες, από τη μια αφορά στην ελευθερία της ανταπόκρισης και της επικοινωνίας και από την άλλη αφορά στο απόρρητο όλων των επιμέρους μορφών επικοινωνίας[55].

Η προστασία του ως άνω άρθρου κατοχυρώνεται στο πλαίσιο που αυτή λαμβάνει χώρα σε καθεστώς εμπιστευτικότητας, ήτοι δεν έχει ως σκοπό τη δημοσιοποίηση αλλά, αντίθετα, οι επικοινωνούντες επιθυμούν να παραμείνει γνωστή αποκλειστικά μεταξύ τους. Δεν έχει δε σημασία για την προστασία του απορρήτου εάν η επικοινωνία διεξάγεται εξ αποστάσεως ή εκ του σύνεγγυς. Το άρθρο 19 συνεπικουρείται από το άρθρο 9Α[56] του Συντάγματος περί προστασίας προσωπικών δεδομένων.

---

[51] Άρθρο 14 Σ. 1844: «*Το απόρρητο των επιστολών είναι απαραβίαστον*».

[52] Γ. Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018, σελ. 104.

[53] Αρ. 19 Σ.: «*1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.*

2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1.

3. Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α.»

[54] Αικ. Παπανικολάου, «*Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*», 2020, διαθέσιμο εδώ: http://www.adae.gr/enimerosi/leptomereies/article/aikaterina-a-papanikolaoy-drn-dikigoros-melos-stin/

[55] Αικ. Μαστοροστέργιου, «*Η παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας & της προφορικής συνομιλίας κατ' άρθρο 370Α Π.Κ.*», Διπλωματική Εργασία στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο & Πληροφορική», Φεβρουάριος 2021, διαθέσιμη εδώ: https://dspace.lib.uom.gr/bitstream/2159/25761/3/MastorostergiouAikateriniMsc2021.pdf

[56] Αρ. 9Α Σ.: «*Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.*»

ΙΙΙ.2.2. Η ποινική προστασία του απορρήτου

Τη συνταγματική προστασία του απορρήτου των επικοινωνιών συμπληρώνει η ποινική προστασία του, με το άρθρο 370Α του Ποινικού Κώδικα[57]. Η πρόβλεψη για την προστασία του απορρήτου των τηλεφωνημάτων, πρώτη φορά, έκανε την εμφάνισή του στην ελληνική έννομη τάξη με τον Ν. 1291/1982, ενώ έως τότε στον Ποινικό Κώδικα υπήρχε πρόβλεψη με το άρθρο 250 ΠΚ ποινικών κυρώσεων αναφορικά μόνο με τους τηλεφωνικούς υπαλλήλους[58]. Μέχρι σήμερα, το άρθρο 370Α έχει υποστεί πολλές τροποποιήσεις, γεγονός το οποίο δικαιολογείται από τη διαρκή εξέλιξη των μέσων και τρόπων επικοινωνίας.

Με τον Ν. 3674/2008 λήφθηκαν νομοθετικά μέτρα προς την ενίσχυση του θεσμικού πλαισίου της προστασίας του απορρήτου των τηλεφωνικών επικοινωνιών. Ο νόμος αυτός πλήρωσε το κενό που ανέκυψε σε συνέχεια της αποκάλυψης περίπου 100 τηλεφωνικών υποκλοπών σε βάρος πολιτών και κρατικών λειτουργών, μέχρι και του πρωθυπουργού της χώρας, το έτος 2005[59].

Έτσι, ενισχύθηκε το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, μέσω της θέσπισης συγκεκριμένων υποχρεώσεων από την πλευρά των παρόχων όπως για παράδειγμα η υποχρέωση κατάρτισης και εφαρμογής ειδικού σχεδίου πολιτικής ασφάλειας[60], η υποχρέωση καταγραφής των διαχειριστικών λειτουργιών που επιχειρούνται στο λογισμικό κάθε ψηφιακού κέντρου μεταγωγής[61] κ.ά., μέσω της θέσπισης αστικής ευθύνης[62] και της περιγραφής του εθνικού σχεδίου ασφάλειας των επικοινωνιών[63].

Με το άρθρο 9 του νόμου[64] προστέθηκε στον Ποινικό Κώδικα η διάταξη με αριθμό 292Α και τίτλο «*εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών*». Επιπλέον, με το άρθρο 10 του Ν. 3674/2008[65] επήλθε τροποποίηση και διεύρυνση του αξιοποίνου του άρθρου 370Α ΠΚ, με το οποίο προστέθηκε στην αντικειμενική υπόσταση του εγκλήματος της

---

[57] Βλ. άρθρο 370Α ΠΚ: «*Παραβίαση του απορρήτου τηλεφωνικής επικοινωνίας και προφορικής συνομιλίας*»
[58] Βλ. άρθρο 250 καταργηθέντος με τον Ν. 4619/2019 ΠΚ «*Παραβάσεις των τηλεφωνικών υπαλλήλων*».
[59] Ιωάννης Δημ. Ιγγλεζάκης «Δίκαιο Πληροφορικής», Εκδόσεις Σάκκουλα, 2018, σελ. 310.
[60] Βλ. άρθρο 3 Ν. 3674/2008 «*Ειδικό σχέδιο πολιτικής ασφάλειας*».
[61] Βλ. άρθρο 5 Ν. 3674/2008 «*Καταγραφή διαχειριστικών λειτουργιών*».
[62] Βλ. άρθρο 12 Ν. 3674/2008 «*Αστική Ευθύνη*».
[63] Βλ. άρθρο 13 Ν. 3674/2008 «*Εθνικό σχέδιο ασφάλειας ηλεκτρονικών επικοινωνιών*».
[64] Βλ. άρθρο 9 Ν. 3674/2008 «*Τροποποιήσεις και προσθήκη άρθρου 292Α στον Ποινικό Κώδικα*».
[65] Βλ. άρθρο 10 Ν. 3674/2008 «*Τροποποίηση του άρθρου 370Α του Ποινικού Κώδικα*».

παραβίασης του απορρήτου των τηλεφωνικών επικοινωνιών η αθέμιτη παρέμβαση σε «*δίκτυο παροχής υπηρεσιών τηλεφωνίας ή σε σύστημα υλικού ή λογισμικού*»[66].

Η ποινική προστασία του απορρήτου των επικοινωνιών και συνεπώς της ιδιωτικής ζωής του ατόμου που εκφράζεται μέσω της επικοινωνίας, καταδεικνύει τη μεγάλη σημασία της πραγματικής προστασίας του αγαθού αυτού, την οποία ο νομοθέτης προσπαθεί να επιτύχει με τις διαρκείς τροποποιήσεις του άρθρου 370Α ΠΚ, ώστε να εναρμονίζεται η διάταξη αυτή με τα σύγχρονα τεχνολογικά δεδομένα.

ΙΙΙ.2.3. Ο Ν. 3115/2003

Με το άρθρο 1 του Ν. 3115/2003, κατ' επιταγή του άρθρου 19 § 2 του Συντάγματος, συστάθηκε η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, η οποία έχει ως σκοπό της «*την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών*» ενώ στην έννοια της προστασίας περιλαμβάνεται και «*ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου*»[67].

ΙΙΙ.2.4. Λοιποί νόμοι στην ελληνική έννομη τάξη

Αρκετοί, ακόμη, νόμοι υιοθετήθηκαν από τον Έλληνα νομοθέτη, με σκοπό την αποτελεσματική προστασία του απορρήτου των επικοινωνιών, όπως είναι ο Ν. 3431/2006 «*Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις*» και ο Ν. 3471/2006, όπως τροποποιήθηκε με τον Ν. 4070/2012, με τον οποίο, όπως αναφέρθηκε και ανωτέρω (βλ. ανωτέρω παράγραφο ΙΙΙ.1.3.), ενσωματώθηκε στην ελληνική έννομη τάξη η ePrivacy Directive, και έχει ως σκοπό την προστασία των θεμελιωδών δικαιωμάτων των προσώπων και κυρίως της ιδιωτικής τους ζωής καθώς και τη θέσπιση των προϋποθέσεων εκείνων που θα συμβάλλουν στην ορθή επεξεργασία των δεδομένων προσωπικού χαρακτήρα και στη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών[68].

ΙΙΙ.3. Οι περιορισμοί στο δικαίωμα της προστασίας του απορρήτου

---

[66] Γ. Τσόλιας, «*Η ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας σύμφωνα με τον Ν 3674/2008 (Παρουσίαση και ερμηνευτική προσέγγιση των διατάξεων)*», Νομική Βιβλιοθήκη, ΔiΜΕΕ, 3/2008, σελ. 334- 352.

[67] Βλ. αναλυτικότερα: http://www.adae.gr/i-adae/paroysiasi/

[68] Βλ. άρθρο 1 Ν. 3471/2006.

Παρά το γεγονός ότι σύμφωνα με το άρθρο 19 § 1 εδ. 1 του Συντάγματος γίνεται λόγος για «*απόλυτα απαραβίαστο*» δικαίωμα, ως λέχθηκε και ανωτέρω, στο αμέσως επόμενο εδάφιο γίνεται λόγος για περιορισμό του δικαιώματος «*για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων*». Η άρση του απορρήτου που βασίζεται στους δύο αυτούς λόγους είναι επιτρεπτή, μόνο στην περίπτωση που διαταχθεί με τις απαραίτητες εγγυήσεις της δικαστικής εξουσίας, όπως επιτάσσει η ίδια η συνταγματική διάταξη. Παρά το ως άνω παράδοξο, το οποίο φαίνεται να καταδεικνύει ότι εντέλει το δικαίωμα της προστασίας του απορρήτου δεν είναι απολύτως απαραβίαστο, ωστόσο, δεν είναι αυτό ικανό να κλονίσει τον υψηλό συμβολισμό του υπό προστασία δικαιώματος στην αξιακή κλίμακα του δημοκρατικού μας πολιτεύματος[69].

Σε συνέχεια, επομένως, της συνταγματικής επιταγής υιοθετήθηκε ο Ν. 2225/1994, δυνάμει του οποίου θεσπίστηκε οργανωτικά η διαδικασία της άρσης του απορρήτου για τους ανωτέρω λόγους. Ειδικότερα, με το άρθρο 3[70] σε συνδυασμό με το άρθρο 5[71] ορίστηκε η διαδικασία της άρσης για λόγους εθνικής ασφάλειας, οι οποίοι όμως δεν ορίζονται ρητά, και στο άρθρο 4[72] εισάγεται ο κατάλογος των «*ιδιαίτερα σοβαρών εγκλημάτων*», για τη διακρίβωση των οποίων αποκλειστικά μπορεί να ακολουθηθεί η διαδικασία της άρσης του απορρήτου[73].

Επιπλέον, με το ΠΔ με αριθμό 47/2005 ορίστηκαν οι «*Διαδικασίες καθώς και οι τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του*». Πιο συγκεκριμένα, καθορίστηκαν τα είδη της επικοινωνίας στα οποία έχει εφαρμογή η άρση του απορρήτου με την παράλληλη επέκταση του απορρήτου και στις επικοινωνίες μέσω

---

[69] Αικ. Παπανικολάου, «*Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*», 2020, σελ. 5.

[70] Βλ. άρθρο 3 Ν. 2225/1994 «*Άρση του απορρήτου για λόγους εθνικής ασφάλειας*».

[71] Βλ. άρθρο 5 Ν. 2225/1994 «*Διαδικασία άρσης του απορρήτου*».

[72] Βλ. άρθρο 4 Ν. 2225/1994 «*Άρση του απορρήτου για διακρίβωση εγκλημάτων*».

[73] Με το άρθρο 43 του Ν. 4640/2019 (ΦΕΚ Α' 190/30.11.2019) , παντελώς αιφνιδιαστικά εισήχθη στο άρθρο 34 παρ. 1 του ΚΠΔ η εξής προσθήκη: «*ειδικώς η πρόσβαση σε κάθε πληροφορία ή στοιχείο του τηλεπικοινωνιακού απορρήτου (ν. 2225/1994) επιτρέπεται σε περιπτώσεις κατά τις οποίες αποτυπώνεται και τεκμηριώνεται η αντικειμενική υπόσταση κακουργήματος*». Δυνάμει της τροποποίησης αυτής προστέθηκαν στον περιοριστικό πίνακα των εγκλημάτων του Ν. 2225/1994 και οι περιπτώσεις εγκλημάτων κατά τα οποία αποτυπώνεται και τεκμηριώνεται η αντικειμενική υπόσταση κακουργήματος οικονομικής φύσης, χωρίς όμως αυτά να απαριθμούνται περιοριστικά. Οι αντιδράσεις που επέφερε η βουλευτική τροπολογία αυτή ήταν πολλές με αποτέλεσμα να αντικατασταθεί το άρθρο ως ισχύει σήμερα, ήτοι χωρίς την αμφιλεγόμενη ως άνω διάταξη, δυνάμει του άρθρου 53 παρ. 3 Ν. 4745/2020 (ΦΕΚ Α' 214/06.11.2020). Βλ. σχετικά άρθρο Αικατερίνας Παπανικολάου, «*Ανησυχία από το νέο καθεστώς άρσης απορρήτου*», Εφημερίδα «ΤΑ ΝΕΑ», 16 Δεκέμβριου 2019.

διαδικτύου[74][75], τα στοιχεία στα οποία επιτρέπεται η πρόσβαση[76], καθορίστηκε το είδος του τεχνολογικού εξοπλισμού που θα χρησιμοποιηθεί για την άρση[77], τα μέσα και η μέθοδος της πρόσβασης στα ως άνω στοιχεία[78] καθώς και οι υποχρεώσεις των παρόχων υπηρεσιών και δικτύων[79].

Εντούτοις, η ΑΔΑΕ με την Έκθεση Πεπραγμένων της για το έτος 2020 σημείωσε ότι με τις ραγδαίες τεχνολογικές εξελίξεις που λαμβάνουν χώρα και δη από τη συνεχή ανάπτυξη των τεχνολογιών παρακολούθησης, το απόρρητο βρίσκεται σε διαρκή κίνδυνο. Πολλώ δε μάλλον στην Έκθεση αναφέρεται ότι σε όλες τις χώρες αλλά και στην Ελλάδα παρατηρείται μια αρκετά εντυπωσιακή άνοδος του αριθμού των «νομίμων παρακολουθήσεων» των επικοινωνιών των πολιτών, ήτοι των παρακολουθήσεων, οι οποίες βασίζονται σε μια νόμιμη διαδικασία (συνήθως λαμβάνουν χώρα ύστερα από αίτηση μιας δημόσιας υπηρεσίας και έγκρισή της από την αρμόδια δικαστική αρχή)[80]. Οι παρακολουθήσεις αυτές κατά βάση «δικαιολογούνται» από την ανάγκη καταπολέμησης της τρομοκρατίας, της βαριάς εγκληματικότητας κ.λπ. Όμως, πάντοτε ελλοχεύει ο κίνδυνος κατάχρησης από τα κρατικά όργανα των εξαιρέσεων που θεσπίζονται από τον ίδιο τον συνταγματικό νομοθέτη.

Η ως άνω διαπίστωση της ΑΔΑΕ έχει μεγάλη σημασία, εάν εξεταστεί σε συνάρτηση με την τροποποίηση του άρθρου 5 Ν. 2225/1994 με το άρθρο 87 Ν. 4790/2021[81]. Όπως έχει διαμορφωθεί πλέον το άρθρο 5 § 9 ορίζει ότι: «*Στις περιπτώσεις του άρθρου 4, η Α.Δ.Α.Ε. δύναται, μετά τη λήξη του μέτρου της άρσης, να αποφασίζει τη γνωστοποίηση της επιβολής του μέτρου αυτού στους θιγόμενους, με τη σύμφωνη γνώμη του Εισαγγελέα του Αρείου Πάγου και υπό την προϋπόθεση, ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε […] Η παρούσα δεν εφαρμόζεται σε περιπτώσεις άρσης του απορρήτου για λόγους εθνικής ασφάλειας, σύμφωνα με*

---

[74] Σε σύγκρουση με τη διάταξη αυτή έρχεται η περίφημη Γνωμοδότηση με αριθμό 9/2009 του εισαγγελέα του Αρείου Πάγου, Σανιδά, ο οποίος υποστήριξε σθεναρά ότι το απόρρητο των επικοινωνιών δεν μπορεί να καλύπτει την επικοινωνία μέσω του διαδικτύου, διότι προχωρώντας σε αυτή τη μορφή επικοινωνίας, τα μέρη αποδέχονται τη δημοσιότητά της και άρα σε περίπτωση τέλεσης κάποιου σχετιζόμενου αδικήματος, δεν απαιτείται η τήρηση των διατάξεων περί άρσης του απορρήτου.

[75] Βλ. άρθρο 3 ΠΔ 47/2005 «*Είδη Επικοινωνίας*».

[76] Βλ. άρθρο 4 ΠΔ 47/2005 «*Στοιχεία Επικοινωνίας*».

[77] Βλ. άρθρο 6 ΠΔ 47/2005 «*Εξοπλισμός*».

[78] Βλ. άρθρο 7 ΠΔ 47/2005 «*Μέσα και Μέθοδοι*».

[79] Βλ. άρθρο 8 ΠΔ 47/2005 «*Υποχρεώσεις των παρόχων υπηρεσιών και δικτύων*»

[80] Βλ. αναλυτικά Έκθεση Πεπραγμένων ΑΔΑΕ για το έτος 2020, διαθέσιμη εδώ: http://www.adae.gr/fileadmin/docs/pepragmena/2020/EKTHESI_2020.pdf

[81] Ν. 4790/2021 «Κατεπείγουσες ρυθμίσεις για την προστασία δημόσιας υγείας από τις συνεχιζόμενες συνέπειες της πανδημίας του κορωνοϊού COVID-19, την ανάπτυξη, την κοινωνική προστασία και την επαναλειτουργία των δικαστηρίων και άλλα ζητήματα».

το άρθρο 3.». Καταργήθηκε, άρα, η αρμοδιότητα της ΑΔΑΕ να γνωστοποιεί την άρση του απορρήτου που έλαβε χώρα στον ενδιαφερόμενο, μετά τη λήξη της, εάν η άρση αυτή δικαιολογείται από «*λόγους εθνικής ασφάλειας*», γεγονός που πιθανότατα καθιστά την τροποποιητική αυτή διάταξη ασύμβατη με το Σύνταγμα και ειδικότερα με το άρθρο 19 § 1.[82]

Συνεπώς, γίνεται αντιληπτό ότι η άρση του απορρήτου, καταρχήν, θα πρέπει να γίνεται ως **ultimum refugium** και πάντοτε τηρώντας την ισχύουσα νομοθεσία σε συνάρτηση με τη θεμελιώδη αρχή της αναλογικότητας, δεδομένου μάλιστα ότι το ποινικό δικονομικό δίκαιο δεν βασίζει την αναζήτηση ή την αποκάλυψη της αλήθειας σε αθέμιτες και παράνομες πρακτικές[83].

[82] Βλ. αναλυτικά την επιστημονική άποψη του Προέδρου και των δύο μελών της ΑΔΑΕ σε σχέση με τα προβλήματα συμβατότητας της πρόσφατης διάταξης του άρθρου 87 του Ν. 4790/2021 με υπέρτερης τυπικής ισχύος κανόνες δικαίου, διαθέσιμη εδώ: https://www.lawspot.gr/nomika-nea/aporrito-epikoinonion-antithesi-toy-arthroy-87-n-4790-2021-pros-tis-eggyiseis-tis

[83] Γ. Ζέκος, «*Διαδίκτυο, Η/Υ & Τηλεπικοινωνίες στο Ελληνικό Δίκαιο*», Εκδόσεις Σάκκουλα, 2017, σελ. 417.

IV. Ο ΚΑΝΟΝΙΣΜΟΣ ePRIVACY ΩΣ ΝΕΟ ΝΟΜΟΘΕΤΗΜΑ

IV.1. Τι είναι ο ePrivacy και ποιο είναι το κενό που θα καλύψει;

Ο υπό εξέταση Κανονισμός και το πολυαναμενόμενο τελικό του κείμενο, όπως αναφέρθηκε και στην Εισαγωγή (βλ. ανωτέρω παράγραφο Ι.), τροποποιούν και εισάγουν μια σειρά από εξαιρετικά κρίσιμες διατάξεις, αφορώσες στην προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Οι διατάξεις αυτές «υπόσχονται» να ρυθμίσουν με τρόπο ομοιόμορφο, συνεκτικό και υποχρεωτικό[84] το πεδίο των ηλεκτρονικών επικοινωνιών όσον αφορά στην προστασία του απορρήτου και των δεδομένων των επικοινωνιών των τελικών χρηστών, σε όλα τα κράτη- μέλη της Ένωσης, αίροντας με τον τρόπο αυτό οποιαδήποτε σύγχυση υφίσταται σήμερα στην εκάστοτε εθνική νομοθεσία και νομολογία.

Ταυτόχρονα με την ψήφιση του Κανονισμού, θα επέλθει η κατάργηση της οδηγίας 2002/58/ΕΚ, γεγονός, όμως, που σε καμία περίπτωση δεν σημαίνει ότι οι αρχές που θεσπίζει και οι διατάξεις της είναι λανθασμένες. Ωστόσο, η οδηγία δεν ήταν δυνατό να συμβαδίσει, ως καθίσταται πλέον απαραίτητο, με την ραγδαία εξέλιξη των τεχνολογικών μέσων και την κατάσταση που επικρατεί στην αγορά, γεγονός το οποίο είχε το δυσμενές αποτέλεσμα της έλλειψης συνοχής ή/ και της ανεπάρκειας όσον αφορά στην προστασία του απορρήτου των επικοινωνιών.

Οι διατάξεις του Κανονισμού αποτελούν εξειδίκευση και συμπλήρωση των άρθρων του ΓΚΠΔ, που αφορούν στα δεδομένα ηλεκτρονικών επικοινωνιών, τα οποία ανταποκρίνονται στον ορισμό των δεδομένων προσωπικού χαρακτήρα. Βέβαια, σε αντίθεση με τον ΓΚΠΔ, ο Κανονισμός θα έχει εφαρμογή τόσο στα φυσικά όσο και στα νομικά πρόσωπα[85].

Έτσι, ο Κανονισμός επιδιώκει να ρυθμίσει τις περιπτώσεις κατά τις οποίες οι πάροχοι των υπηρεσιών ηλεκτρονικών επικοινωνιών αλλά και οι πάροχοι δημόσιων καταλόγων θα δύνανται να επεξεργάζονται δεδομένα (ήτοι περιεχόμενο και μεταδεδομένα[86]) μιας επικοινωνίας ή να έχουν πρόσβαση σε πληροφορίες που βρίσκονται αποθηκευμένες στον τερματικό εξοπλισμό του τελικού χρήστη. Ακόμη, αποπειράται να ρυθμίσει και τη

[84] Γρ. Τσόλιας, «*Εξελίξεις στον τομέα της επιτήρησης των ηλεκτρονικών επικοινωνιών: από την Ασφάλεια στην Ελευθερία και τη διεύρυνση της προστατευόμενης επικοινωνίας*», Ποινική Δικαιοσύνη, Νομική Βιβλιοθήκη, Τευχ. 8- 9, Αύγουστος- Σεπτέμβριος, 2017, σελ. 791.

[85] Βλ. αιτιολογική σκέψη με αριθμό 1 του Σχεδίου 02.2021 του Κανονισμού.

[86] Βλ. άρθρο 4 § 3 περ. α' του σχεδίου 02.2021 του Κανονισμού περί ορισμού των δεδομένων της ηλεκτρονικής επικοινωνίας.

συμπεριφορά φυσικών και νομικών προσώπων, τα οποία χρησιμοποιούν τις εν λόγω υπηρεσίες με σκοπό την προώθηση υπηρεσιών/ προϊόντων ή με σκοπό την πρόσβαση σε πληροφορίες που βρίσκονται αποθηκευμένες στον τερματικό εξοπλισμό του τελικού χρήστη[87].

Σημαντικό είναι το γεγονός ότι ο Κανονισμός θα εφαρμόζεται πέραν των έως πριν λίγα χρόνια συνηθισμένων μορφών επικοινωνίας. Ειδικότερα, ο Κανονισμός θα αφορά όχι μόνο τους παρόχους σταθερής και κινητής τηλεφωνίας αλλά και τις «*κομβικές υπηρεσίες στην εποχή της 4ης Βιομηχανικής Επανάστασης*» [88] , τις λεγόμενες «ανταγωνιστικές» υπηρεσίες επικοινωνίας[89], τις επικοινωνίες μεταξύ συσκευών/ μηχανών που συνδέονται μεταξύ τους και ανταλλάσσουν δεδομένα και πληροφορίες[90] (Διαδίκτυο των Πραγμάτων/ Internet of Things) καθώς και τα ασύρματα δίκτυα, τα οποία είναι δημόσια ή ημιδημόσια[91].

IV.2. Οι ειδικότερες έννοιες που εντοπίζονται στον Κανονισμό

IV.2.1. Το περιεχόμενο της επικοινωνίας

Στην έννοια του περιεχομένου της επικοινωνίας εμπίπτει το ίδιο το μήνυμα, ήτοι η ίδια η πληροφορία η οποία μεταδίδεται και έχει ως σκοπό αυτή καθ' εαυτή την πραγματοποίηση της επικοινωνίας με οποιονδήποτε τρόπο και αν αυτή λαμβάνει χώρα[92], είτε προφορικά μέσω τηλεφώνου, είτε μέσω SMS, είτε με την αποστολή μιας φωτογραφίας, είτε μέσω ηλεκτρονικού ταχυδρομείου κ.λπ.

Από το ίδιο το περιεχόμενο της επικοινωνίας, δηλαδή από το μήνυμα το οποίο μεταφέρεται από τον έναν χρήστη στον άλλον, είναι δυνατό να προκύπτουν προσωπικές πληροφορίες που αφορούν ένα συγκεκριμένο άτομο αλλά ακόμη και εξαιρετικά ευαίσθητες πληροφορίες, όπως είναι η κατάσταση της υγείας του, η θρησκεία του κ.ά. Καθίσταται άρα επιτακτική, χωρίς αμφιβολία, η προστασία του περιεχομένου της επικοινωνίας, στην οποία

---

[87] Βλ. αιτιολογική σκέψη με αριθμό 8 του Σχεδίου 02.2021 του Κανονισμού.

[88] Σχόλιο του Ν. Κανελλόπουλου, διαθέσιμο εδώ: https://lawyermagazine.gr/the-eprivacy-saga-to-xroniko-gia-thn-psifisi-enos-kanonismou/

[89] Παρουσίαση της ΑΠΔΠΧ από την 11η Ευρωπαϊκή Ημέρα Προστασίας Προσωπικών Δεδομένων, «*Η Εμπειρία από την εφαρμογή της νομοθεσίας για την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες, Εν όψει της αναθεώρησης της οδηγίας e-Privacy (2002/58/ΕΚ)*», 28.01.2017, διαθέσιμη εδώ: https://www.dpa.gr/sites/default/files/2019-11/e-privacy-gr-final-3.pdf?fbclid=IwAR3JY2MQQc99SPGkd9UOsOm68rmDTEgL0h_gVjbBTxPJIaEQZOPhCjTjjb4

[90] Βλ. αιτιολογική σκέψη με αριθμό 12 του Σχεδίου 02.2021 του Κανονισμού

[91] Βλ. αιτιολογική σκέψη με αριθμό 12 του Σχεδίου 02.2021 του Κανονισμού.

[92] Γρ. Τσόλιας, «*Η προστασία του απορρήτου των επικοινωνιών κατά το ΠΔ 47/2005 (Βασικά χαρακτηριστικά και σύντομη ερμηνευτική προσέγγιση)*», Νομική Βιβλιοθήκη, ΔΙΤΕ, 2/2005.

προχωρά και ο υπό μελέτη Κανονισμός με τα άρθρα 5, 6 και 6α, όπως θα αναλυθούν εκτενώς κατωτέρω.

IV.2.2. Τα μεταδεδομένα της επικοινωνίας

Μέχρι την εφαρμογή του Κανονισμού, παραδοσιακά, η ισχύουσα έννομη τάξη τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, διακρίνει το περιεχόμενο της επικοινωνίας από τα λεγόμενα «εξωτερικά της στοιχεία». Εντούτοις, ο Κανονισμός με την αιτιολογική του σκέψη με αριθμό 1 εντάσσει στο απόρρητο των επικοινωνιών τόσο την ίδια την πληροφορία που μεταδίδεται από τα επικοινωνούντα μέρη όσο και τα εξωτερικά στοιχεία της επικοινωνίας.

Ειδικότερα, με τον όρο «εξωτερικά στοιχεία της επικοινωνίας» ορίζονται τα δεδομένα κίνησης και θέσης. Ως δεδομένα κίνησης, σύμφωνα με το άρθρο 2 § 3 του Ν. 3471/2006 ορίζονται: «*τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία*». Επίσης, σύμφωνα με το άρθρο 2 § 4 του ίδιου νόμου δόθηκε και ο ορισμός των δεδομένων θέσης, σύμφωνα με το οποίο: «*τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μίας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών*».

Με τον υπό μελέτη Κανονισμό, εντούτοις, ο όρος «εξωτερικά στοιχεία» εξαλείφεται και πλέον μετατρέπονται σε «μεταδεδομένα» της επικοινωνίας ενώ το σύνολο της γενόμενης επικοινωνίας, συμπεριλαμβανομένου του περιεχομένου και των μεταδεδομένων της επικοινωνίας εμφανίζεται ως «δεδομένα ηλεκτρονικών επικοινωνιών»[93].

Ο Κανονισμός επεκτείνει, σε σχέση με την οδηγία 2002/58/ΕΚ, τις δυνατότητες των παρόχων των ηλεκτρονικών επικοινωνιών να επεξεργάζονται τα μεταδεδομένα, ενισχύοντας παράλληλα όμως και το προστατευτικό τους πλαίσιο. Η επεξεργασία των μεταδεδομένων θα πρέπει πάντοτε να διαδέχεται τη συγκατάθεση του τελικού χρήστη καθώς και η επεξεργασία

[93] Βλ. Άρθρο 4 περ. (α), (β) και (γ) του Σχεδίου 02.2021 του Κανονισμού.

τους να είναι πάντοτε συμβατή με τους λόγους για τους οποίους εξ αρχής συλλέχθησαν[94]. Η εκτεταμένη αυτή προστασία τους δικαιολογείται διότι τα μεταδεδομένα, τα οποία προκύπτουν από τις ηλεκτρονικές επικοινωνίες και αφορούν για παράδειγμα τους κληθέντες αριθμούς ενός χρήστη, τους δικτυακούς τόπους τους οποίους επισκέφθηκε ο χρήστης, τη γεωγραφική του θέση, τη διάρκεια μιας κλήσης κ.λπ. υπάρχει πιθανότητα να αποκαλύπτουν πολύ πιο σημαντικές προσωπικές ή/ και ευαίσθητες πληροφορίες σε σχέση με το ίδιο το περιεχόμενο της επικοινωνίας.

IV.2.2.1. Η θέση της νομοθεσίας αναφορικά με την προστασίας των εξωτερικών στοιχείων της επικοινωνίας

Αξιοσημείωτος όσον αφορά στα εξωτερικά στοιχεία της επικοινωνίας είναι ο τρόπος με τον οποίο αντιμετωπίζονται από τη νομοθεσία και τη νομολογία σε ευρωπαϊκό αλλά και σε εγχώριο επίπεδο.

Ήδη με το ΠΔ 47/2005 θεωρήθηκε ότι λύθηκε το ζήτημα της υπαγωγής ή μη των εξωτερικών στοιχείων της επικοινωνίας στην προστασία του απορρήτου της επικοινωνίας, αφού προστέθηκαν ρητά στο προστατευτικό του πλαίσιο[95]. Επίσης, με τις διατάξεις της οδηγίας 2002/58/ΕΚ, όπως υιοθετήθηκαν από την ελληνική έννομη τάξη με τον Ν. 3471/2006[96], ρητά προστατεύθηκε οποιαδήποτε επικοινωνία, συμπεριλαμβανομένων και των δεδομένων κίνησης και θέσης[97], που λαμβάνει χώρα μέσω δημόσιου δικτύου και μέσω των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

Επίσης, και ο υπό μελέτη Κανονισμός αντιμετωπίζει τα μεταδεδομένα ως άξια προστασίας, δεδομένου ότι από τη συλλογή τους μπορούν να εξαχθούν ασφαλή συμπεράσματα για την ιδιωτική ζωή του χρήστη[98] και παράλληλα διευρύνει τις δυνατότητες επεξεργασίας τους από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών σε σχέση με την υπό κατάργηση οδηγία, 2002/58/ΕΚ.

---

[94] Βλ. Αιτιολογικές Σκέψεις 17 και 17aa του Σχεδίου 02/2021 του Κανονισμού. Για τις εξαιρετικές περιπτώσεις επεξεργασίας των μεταδεδομένων βλ. Αιτιολογικές Σκέψεις 17a, 17b και 18.

[95] Βλ. αναλυτικά τα Άρθρα 3 και 4 του ΠΔ 47/2005.

[96] Βλ. αναλυτικά το Άρθρο 4 του Ν. 3471/2006.

[97] Π. Κίτσος, «*Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών. Ενσωμάτωση των ρυθμίσεων της Ευρωπαϊκής Ένωσης στο ελληνικό δίκαιο*», Διδακτορική Διατριβή στο Πανεπιστήμιο Μακεδονίας Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Εφαρμοσμένης Πληροφορικής, Θεσσαλονίκη 2011, διαθέσιμη εδώ: https://dspace.lib.uom.gr/bitstream/2159/14739/2/Kitsos_Phd2011.pdf

[98] Βλ. Αιτιολογική Σκέψη 2 του σχεδίου 02/2021 του Κανονισμού.

IV.2.2.2. Η θέση του Αρείου Πάγου αναφορικά με την προστασίας των εξωτερικών στοιχείων της επικοινωνίας

Σταθερή προς την αντίθετη κατεύθυνση εμφανίζεται η κρίση του Αρείου Πάγου. Ο τέως Εισαγγελέας του Ανωτάτου Ακυρωτικού Δικαστηρίου της χώρας, κ. Γεώργιος Σανιδάς,3 κατά το έτος 2009 εξέδωσε τη με αριθμό 9/2009 γνωμοδότησή του[99] προς το 5ο τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος, σύμφωνα με την οποία το απόρρητο των επικοινωνιών δεν καλύπτει τις επικοινωνίες που λαμβάνουν χώρα μέσω διαδικτύου αλλά ούτε και τα εξωτερικά στοιχεία της επικοινωνίας. Πολλώ δε μάλλον κατέληξε στο συμπέρασμα ότι «*οι εισαγγελικές, ανακριτικές και προανακριτικές αρχές, πολύ δε περισσότερο τα δικαστικά συμβούλια και τα δικαστήρια, στα πλαίσια των ερευνών για τη διακρίβωση τελέσεως ενός εγκλήματος και του δράστη, δικαιούνται να ζητούν από τους παρόχους των υπηρεσιών επικοινωνίας μέσω του Internet τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξεως, την ημεροχρονολογία και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος και ο πάροχος υποχρεούται να τα παραδίδει χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιας αρχής και ιδία της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών*»[100]. Παρομοίως έχουν κρίνει και ορισμένα ποινικά τμήματα του Αρείου Πάγου με σχετικές αποφάσεις τους[101].

Το Συμβούλιο της Επικρατείας έκρινε παντελώς αντίθετα σε σχέση με τον Άρειο Πάγο. Το Ανώτατο Διοικητικό Δικαστήριο της χώρας έκρινε με τη με αριθμό 1593/2016 απόφαση του Δ' τμήματός του[102] ότι τα εξωτερικά στοιχεία της επικοινωνίας, τα οποία βρίσκονται αποθηκευμένα στον τερματικό εξοπλισμό του χρήστη, επομένως πρόκειται για παρελθοντικά στοιχεία και για επικοινωνία που δεν λαμβάνει χώρα τη δεδομένη στιγμή, χρήζουν, επίσης, προστασίας και άρα για τη χορήγηση σχετικών πληροφοριών από την πλευρά των παρόχων στις εισαγγελικές και δικαστικές αρχές της χώρας, οι τελευταίες οφείλουν να τηρούν τα όσα

---

[99] Διαθέσιμο το πλήρες κείμενο της Γνωμοδότησης εδώ: https://eisap.gr/%ce%b3%ce%bd%cf%89%ce%bc%ce%bf%ce%b4%cf%8c%cf%84%ce%b7%cf%83%ce%b7-09-2009/

[100] Προς αυτή την κατεύθυνση κινήθηκαν και ο Εισαγγελέας του Αρείου Πάγου, Ι. Τέντες, με τη γνωμοδότησή του με αριθμό 12/2009, η οποία ουσιαστικά επικύρωσε τη γνωμοδότηση του Σανιδά και ο Αντιεισαγγελέας του Αρείου Πάγου, Α. Κατσιδώρης με τη με αριθμό 09/2011 γνωμοδότησή του.

[101] Βλ. ενδεικτικά ΑΠ 711/2011 ΠοινΔικ 2012, 518, ΑΠ 203/2014 ΠοινΧρ 2015, 103 επ.

[102] Διαθέσιμο το πλήρες κείμενο της απόφασης εδώ: http://www.adjustice.gr/webcenter/portal/ste/ypiresies/nomologies?_afrLoop=33866166662155739#!%40%40%3F_afrLoop%3D33866166662155739%26centerWidth%3D65%2525%26leftWidth%3D0%2525%26npath%3D%252Fwebcenter%252Fportal%252Fste%252Fypiresies%252Fnomologies%26rigthWidth%3D35%2525%26showFooter%3Dfalse%26showHeader%3Dtrue%26_adf.ctrl-state%3Dkj8fgltcw_29

ορίζονται από τον Ν. 2225/1994 περί άρσης του απορρήτου των επικοινωνιών. Ειδικότερα, με την ενδέκατη σκέψη του το ΣτΕ ανέφερε τα εξής: «*οι πάροχοι τηλεπικοινωνιακών υπηρεσιών οφείλουν, κατά την άσκηση των δραστηριοτήτων τους, να διασφαλίζουν το απόρρητο της τηλεφωνικής επικοινωνίας και δεν επιτρέπεται να παρέχουν δυνατότητα πρόσβασης στο περιεχόμενο και τα δεδομένα της επικοινωνίας ούτε να γνωστοποιούν σχετικά στοιχεία, παρά μόνο αν εκδοθεί, με τη διαδικασία που ορίζεται στον Ν. 2225/1994, διάταξη άρσης του απορρήτου α) από το αρμόδιο δικαστικό Συμβούλιο Εφετών ή Πλημμελειοδικών ή β) σε εξαιρετικά επείγουσες περιπτώσεις από τον Εισαγγελέα που διενεργεί προανακριτική εξέταση ή τον Ανακριτή που διενεργεί την ανάκριση. Προκειμένου δε οι πάροχοι να εκτελέσουν διάταξη άρσης του απορρήτου θα πρέπει να προκύπτει σαφώς από το ίδιο το σώμα της διατάξεως, με μνεία των σχετικών άρθρων, ότι αυτή εκδόθηκε βάσει των ειδικών διατάξεων του Ν 2225/1994, που διέπουν τη διαδικασία άρσης του απορρήτου της τηλεφωνικής επικοινωνίας*».

Με την απόφαση αυτή θεωρήθηκε ότι λύθηκε εξ ολοκλήρου, σε ερμηνευτικό επίπεδο, η διχογνωμία που είχε δημιουργηθεί κυρίως λόγω της αντίθετης άποψης του Αρείου Πάγου, σχετικά με την προστασία των εξωτερικών στοιχείων της επικοινωνίας στο πλαίσιο της προστασίας του απορρήτων των επικοινωνιών[103]. Την ίδια στάση υπέρ της προστασίας των εξωτερικών στοιχείων της επικοινωνίας κράτησε και η ΑΔΑΕ, όπως άλλωστε ήταν λογικό, σύμφωνα και με τη με αριθμό 1/2005 Γνωμοδότησή της[104].

Ωστόσο, η στάση αυτή του Αρείου Πάγου η οποία εκδηλώνεται τόσο με τις γνωμοδοτήσεις των Εισαγγελέων του όσο και με τις αποφάσεις των ποινικών του τμημάτων[105] έρχεται σε πλήρη αντίθεση με την Οδηγία 2002/58/ΕΚ, με τη νομολογία των ευρωπαϊκών δικαστηρίων, τόσο του ΔΕΕ[106], όσο και του ΕΔΔΑ[107] και με το σχέδιο του Κανονισμού φυσικά, το

---

[103] Γρ. Τσόλιας, «*Σημείωμα στην ΣτΕ 1593/2016- Η υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στην διαδικασία άρσης του απορρήτου και η διασφάλισή της από τους Παρόχους*», ΔiΜΕΕ, 4/2016, σελ. 645-650.

[104] Διαθέσιμο το πλήρες κείμενο εδώ: http://www.adae.gr/fileadmin/docs/nomoi/893-2005.pdf

[105] Βλ. ενδεικτικά αποφάσεις με αριθμούς 570/2006 ΑΠ, 711/2011 ΑΠ και 689/2014 ΑΠ.

[106] Βλ. ενδεικτικά υποθέσεις ΔΕΕ C-293/12 και C-594/12 (Digital Rights Ireland κατά Minister for Communications etc.), διαθέσιμη η απόφαση εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:62012CJ0293&from=el και υποθέσεις C-203/15 και C-698/15 (Tele2 Sverige AB κατά Post-och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis) διαθέσιμη η απόφαση εδώ: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EL

[107] Βλ. ενδεικτικά υπόθεση Malone κατά Ηνωμένου Βασιλείου (1984).

οποίο βέβαια δεν έχει ακόμη ψηφισθεί αλλά θα εφαρμοσθεί δεσμευτικά και συνολικά σε όλα τα κράτη- μέλη της Ένωσης και θα δώσει ένα τέλος σε αυτό το παράδοξο που έχει δημιουργηθεί.

IV.2.3. Η προστασία των πληροφοριών στον τερματικό εξοπλισμό του χρήστη

Ο Κανονισμός, στο άρθρο 4 § 1, περ. 3[108], όσον αφορά στον ορισμό του «τερματικού εξοπλισμού» παραπέμπει στο άρθρο 1, περίπτωση 1 της Οδηγίας 2008/63/ΕΚ της Επιτροπής[109].

Σύμφωνα με την αιτιολογική σκέψη με αριθμό 20 του Κανονισμού[110], ο τερματικός εξοπλισμός του χρήστη αλλά και κάθε πληροφορία που σχετίζεται με τη χρήση του, ήτοι κάθε πληροφορία που υπόκειται σε επεξεργασία, αποθηκεύεται ή συλλέγεται από τον τερματικό εξοπλισμό ή κάθε πληροφορία που αποθηκεύεται και χρησιμεύει στη σύνδεση μεταξύ συσκευών ή/ και στη σύνδεση με εξοπλισμό δικτύου, αποτελούν μέρος της ιδιωτικής σφαίρας του χρήστη και φυσικά ως τέτοιο θα πρέπει να προστατεύεται σύμφωνα με τον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ένωσης.

Για τον λόγο αυτό οι πληροφορίες που βρίσκονται αποθηκευμένες στον τερματικό εξοπλισμό του χρήστη θα πρέπει να προστατεύονται, σύμφωνα με το άρθρο 8 του Κανονισμού, και να επιτρέπεται η επεξεργασία τους σε συνέχεια της συγκατάθεσης του χρήστη και πάντοτε για ειδικά ορισμένους και διαφανείς σκοπούς. Η ρύθμιση αυτή αιτιολογείται από το γεγονός ότι σε αυτές τις πληροφορίες πολλές φορές περιέχονται δεδομένα, τα οποία έχουν να κάνουν με πτυχές της προσωπικότητας του φυσικού προσώπου, όπως για παράδειγμα είναι οι φωτογραφίες, η λίστα επαφών του κ.λπ.

Επιπλέον, στον τερματικό εξοπλισμό του χρήστη καταφέρνουν με ποικίλους τρόπους να εισέλθουν διάφορες διατάξεις όπως για παράδειγμα το λεγόμενο «spyware» (κατασκοπευτικά λογισμικά), τα «web bugs» (διαδικτυακοί κοριοί), τα «tracking cookies» (βλ. κατωτέρω στα είδη των cookies- παράγραφο IV.2.4.3.) αλλά και παρόμοιες διατάξεις, οι οποίες συνήθως, χωρίς τη συγκατάθεση του χρήστη, έχουν πρόσβαση σε πληροφορίες ή/ και

---

[108] (c) the definition of 'terminal equipment' in Article 1 (1) of Commission Directive 2008/63/EC;

[109] «εξοπλισμός τερματικών»:

α) κάθε εξοπλισμός που συνδέεται άμεσα ή έμμεσα με την ηλεκτρονική διασύνδεση ενός δημόσιου δικτύου τηλεπικοινωνιών για τη μεταβίβαση, επεξεργασία ή λήψη πληροφοριών· και στις δύο περιπτώσεις, δηλαδή είτε η σύνδεση είναι άμεση είτε είναι έμμεση, μπορεί να γίνει με καλώδιο, οπτικές ίνες ή ηλεκτρομαγνητικά κανάλια· η σύνδεση είναι έμμεση, αν μεταξύ του τερματικού και της ηλεκτρονικής διασύνδεσης του δημόσιου δικτύου παρεμβάλλεται άλλη συσκευή·

β) ο εξοπλισμός επίγειων δορυφορικών σταθμών.

[110] Και την αιτιολογική σκέψη 24 της Οδηγίας 2002/58/ΕΚ.

ανιχνεύουν δραστηριότητες του χρήστη θέτοντας με τον τρόπο αυτό σε κίνδυνο την ιδιωτικότητά του.

Στη διαδικτυακή καθημερινότητα, ωστόσο, πολλές φορές εισέρχονται τέτοιου είδους διατάξεις στον τερματικό εξοπλισμό του χρήστη, με τη συγκατάθεσή του και χρησιμοποιούνται για θεμιτούς σκοπούς. Οι πιο γνωστές διατάξεις, οι οποίες έχουν απασχολήσει τελευταία, όχι μόνο όσους μελετούν την ιδιωτικότητα και τα προσωπικά δεδομένα του χρήστη αλλά και τον ίδιο τον χρήστη λόγω της ολοένα και μεγαλύτερης διάδοσής τους, είναι τα λεγόμενα «cookies», τα οποία θα εξεταστούν εκτενώς κατωτέρω.

IV.2.3.1. Cookies και παρόμοιοι ιχνηλάτες (trackers)

Η χρήση των ιχνηλατών στο διαδίκτυο, εάν και δεν εμφανίστηκε πρόσφατα, αποτελεί τελευταία ένα σημαντικό ζήτημα, το οποίο τυγχάνει να έχει τεχνολογικές, νομικές αλλά και εμπορικές προεκτάσεις[111]. Αφορμή για να μας απασχολήσει το θέμα αυτό ήταν βέβαια η ψήφιση του Κανονισμού για την Προστασία των Προσωπικών Δεδομένων, χωρίς ωστόσο οι ιχνηλάτες να διέπονται αποκλειστικά από το νομικό αυτό πλαίσιο.

IV.2.3.2. Έννοια των cookies

Ο ορισμός των cookies δίδεται πολύ εύστοχα από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία αναφέρει ότι: «*Τα cookies είναι μικρά αρχεία κειμένου με πληροφορίες, τα οποία αποθηκεύονται από τον διακομιστή (server) ενός ιστοτόπου στην τερματική συσκευή (υπολογιστής, κινητό τηλέφωνο κλπ.) ενός επισκέπτη/χρήστη κατά την πλοήγηση σε αυτόν. Ο ιστότοπος ανακτά τις εν λόγω πληροφορίες σε κάθε επίσκεψη προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει σε αυτή (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, κ.λπ.)*»[112].

Ωστόσο, παρά το γεγονός ότι ο ως άνω ορισμός φαίνεται ακριβής, πιο σωστό θα ήταν να συμπεριλαμβάνουμε πάντοτε στην εξίσωση τις διαρκείς εξελίξεις της τεχνολογίας και των χρησιμοποιούμενων κάθε φορά μεθόδων στο διαδίκτυο[113]. Για παράδειγμα, αρχικά, στον ορισμό

---

[111] Β. Καρκατζούνης, «*Google Analytics και προστασία προσωπικών δεδομένων Το ψήφισμα της Συνόδου των Εποπτικών αρχών προστασίας προσωπικών δεδομένων της Γερμανίας (Datenschutzkonferenz της 12.5.2020)*», Επιθεώρηση Δικαίου Πληροφορικής, Τ. 1, 2020, available online: file:///Users/ilianapap/Downloads/7790-20148-1-SM.pdf

[112] Διαθέσιμος ηλεκτρονικά: https://www.dpa.gr/index.php/el/cookies/plirofories/whatis_cookies

[113] Β. Καρκατζούνης, «*Cookies και προστασία δεδομένων προσωπικού χαρακτήρα*», ΔΙΤΕ, 2/2019, σελ. 172.

της Αρχής περιεχόταν ως τερματική συσκευή αποθήκευσης μόνο ο υπολογιστής, ενώ, εν συνεχεία, προστέθηκε και το κινητό τηλέφωνο, ως φαίνεται ανωτέρω, αφού πλέον ο αριθμός των χρηστών που περιηγούνται στο διαδίκτυο μέσω του κινητού τους τηλεφώνου είναι εξαιρετικά μεγάλος. Στη συνέχεια, είναι εύλογο να προστεθούν κι άλλα τεχνολογικά επιτεύγματα, τα οποία αυτή τη στιγμή πιθανότατα να μη γνωρίζουμε καν.

Με τη χρήση των cookies, είναι δυνατό να εντοπίζεται η συσκευή του χρήστη, να καταγράφεται η κίνησή του κ.ά. ανάλογα με το εκάστοτε εργαλείο ανάλυσης δεδομένων που χρησιμοποιεί η ιστοσελίδα την οποία επισκέπτεται ο χρήστης. Η συλλογή τους γίνεται ύστερα από τη ρητή συγκατάθεση του χρήστη και κάθε φορά που ο χρήστης επισκέπτεται την ίδια ιστοσελίδα, το εκάστοτε λογισμικό μπορεί να «θυμηθεί» τις προτιμήσεις του τελικού χρήστη και να προσαρμόσει το περιεχόμενο και τις διαφημίσεις που εμφανίζονται σύμφωνα με τις ανάγκες κάθε χρήστη.

IV.2.3.3. Διακρίσεις των cookies

Τα cookies, πέραν των ειδικότερων διακρίσεών τους, διακρίνονται, αρχικά, σε cookies «πρώτου μέρους», τα οποία είναι αυτά που αποθηκεύονται απευθείας στον τερματικό εξοπλισμό του τελικού χρήστη και αυτά του «τρίτου μέρους», που προέρχονται από έτερο όνομα χώρου (domain name) μέσω της διαδικασίας παραπομπής σε αρχεία JavaScript διαφημιστικών εταιρειών ή/ και τρίτων[114].

Τα cookies ανάλογα με τη λειτουργία που κάθε φορά επιτελούν, διακρίνονται και σε ορισμένες κατηγορίες, οι οποίες είναι οι ακόλουθες: 1. Τα cookies αναδυόμενου παραθύρου[115], 2. Τα cookies τρίτων μερών ή third- party cookies[116], 3. Τα μόνιμα cookies ή persistent cookies[117], 4. Τα cookies συνεδρίας/ προσωρινά cookies ή session cookies[118], 5. Τα cookies παρακολούθησης

[114] Λ. Κανέλλος, «*The GDPR Handbook*», Νομική Βιβλιοθήκη, 2020, σελ. 376.

[115] Τα cookies αναδυόμενου παραθύρου χρησιμεύουν για την αποθήκευση των προτιμήσεων του χρήστη, για τη βελτίωση της λειτουργικότητας του εκάστοτε ιστοτόπου και για την ανάλυση της κίνησης των επισκεπτών του και μπορούν να αναγνωρισθούν αποκλειστικά από τον συγκεκριμένο ιστότοπο.

[116] Τα cookies τρίτων μερών προέρχονται από τρίτους ιστοτόπους, περιεχόμενο των οποίων πιθανόν να προβάλλεται στον αρχικό ιστότοπο.

[117] Τα μόνιμα cookies αποθηκεύονται στη συσκευή του χρήστη και δεν διαγράφονται αυτόματα με τον τερματισμό του προγράμματος περιήγησης- απαιτούν συγκατάθεση.

[118] Τα cookies συνεδρίας λειτουργούν και παραμένουν στη συσκευή του χρήστη κατά τη διάρκεια της επίσκεψής του στον εκάστοτε ιστότοπο και διαγράφονται αυτόματα με τον τερματισμό του προγράμματος περιήγησης του χρήστη- δεν απαιτούν συγκατάθεση.

κίνησης[119], 6. Τα Supercookies[120] και 7. Η βαθιά επιθεώρηση πακέτων δεδομένων ή deep packet inspection[121].

IV.2.3.4. Οι περιπτώσεις όπου επιτρέπεται η επεξεργασία και αποθήκευση πληροφοριών στον τερματικό εξοπλισμό του τελικού χρήστη

Με το άρθρο 5 § 3 της υπό κατάργηση οδηγίας, ορίζεται ότι η αποθήκευση και επεξεργασία των ήδη αποθηκευμένων πληροφοριών στον τερματικό εξοπλισμό του τελικού χρήστη, επιτρέπεται μόνο σε συνέχεια της ρητής του ως προς αυτό συγκατάθεσης. Προβλέπει, ακόμη, και την περίπτωση κατά την οποία επιτρέπεται η αποθήκευση ή πρόσβαση και επεξεργασία, χωρίς τη λήψη ρητής προηγούμενης συγκατάθεσης από τον χρήστη, με μοναδικό όμως σκοπό τη διενέργεια ή τη διευκόλυνση διαβίβασης μιας επικοινωνίας μέσω του δικτύου ηλεκτρονικών επικοινωνιών ή σε περίπτωση που μια τέτοια ενέργεια θα ήταν απαραίτητη για την παροχή υπηρεσίας της Κοινωνίας της Πληροφορίας την οποία έχει αιτηθεί ο ίδιος ο χρήστης.

Εντοπίζοντας την αιτιολογική σκέψη του Κανονισμού με αριθμό 20, παρατηρούμε ότι αναφορικά με την επεξεργασία και αποθήκευση πληροφοριών στον τερματικό εξοπλισμό του τελικού χρήστη, όπως είναι και τα cookies, για να είναι σύννομη μια τέτοια διαδικασία, θα πρέπει ο πάροχος να έχει πρώτα λάβει τη ρητή συγκατάθεση του τελικού χρήστη, είτε να πρόκειται για μια διαδικασία η οποία δικαιολογείται από κάποιον ειδικό σκοπό. Με το άρθρο 8 του Κανονισμού ορίζονται οι περιπτώσεις κατά τις οποίες επιτρέπεται η επεξεργασία και αποθήκευση των πληροφοριών του τερματικού εξοπλισμού του χρήστη.

Επιπλέον, απαγορεύεται και η συλλογή πληροφοριών, οι οποίες εκπέμπονται από τον τερματικό εξοπλισμό του τελικού χρήστη ώστε να μπορεί να πραγματοποιηθεί σύνδεση με έτερη συσκευή ή με εξοπλισμό δικτύου πέραν των περιπτώσεων που η εν λόγω συλλογή πληροφοριών γίνεται στο πλαίσιο της πραγματοποίησης και διατήρησης της σύνδεσης αυτής, που ο τελικός χρήστης έχει δώσει τη συγκατάθεσή του, που είναι απαραίτητη για στατιστικούς σκοπούς, στην περίπτωση όμως αυτή τα δεδομένα πρέπει να ανωνυμοποιούνται ή να

[119] Τα cookies παρακολούθησης κίνησης ομοιάζουν με τα εργαλεία παρακολούθησης κίνησης και θέσης- απαιτούν συγκατάθεση.

[120] Τα Supercookies είναι εξαιρετικά επιθετικά- αναγνωριστικά αρχεία που συνήθως χρησιμοποιούνται για στοχευμένη διαφήμιση.

[121] Η βαθιά επιθεώρηση πακέτων δεδομένων επίσης αποτελεί μια απειλητική τεχνολογία, η οποία χρησιμοποιείται για το φιλτράρισμα και την παρακολούθηση των περιεχομένων των διακινούμενων πακέτων δεδομένων.

σβήνονται αμέσως μόλις εξυπηρετήσουν τον σκοπό τους ή τέλος που είναι απαραίτητη για την παροχή της υπηρεσίας την οποία αιτήθηκε ο ίδιος ο τελικός χρήστης.

IV.2.4. Οι Διαθέσιμοι στο κοινό κατάλογοι

Με το άρθρο 4 § 1 περίπτωση δ' ο Κανονισμός δίνει τον ορισμό του διαθέσιμου στο κοινό καταλόγου αναφέροντας ότι πρόκειται για έντυπο ή ηλεκτρονικό κατάλογο των τελικών χρηστών των υπηρεσιών ηλεκτρονικών υπηρεσιών, ο οποίος είτε δημοσιεύεται είτε τίθεται στη διάθεση του κοινού ή σε μέρος μόνο αυτού και οδηγεί στην ταυτοποίηση των εν λόγω χρηστών.

Έτσι, οι διαθέσιμοι στο κοινό κατάλογοι κατά τον Κανονισμό, όπως εμφαίνεται και από την αιτιολογική σκέψη με αριθμό 30 αυτού, περιέχουν βασικά προσωπικά δεδομένα των τελικών χρηστών, όπως είναι για παράδειγμα οι τηλεφωνικοί τους αριθμοί, οι διευθύνσεις του ηλεκτρονικού τους ταχυδρομείου κ.ά. και διανέμονται σε άγνωστο αριθμό προσώπων.

Καθίσταται, συνεπώς, σαφές ότι οι τελικοί χρήστες θα πρέπει να δίνουν τη συγκατάθεσή τους αναφορικά με τη συμπερίληψή τους σε έναν τέτοιου είδους κατάλογο ο οποίος είναι διαθέσιμος στο κοινό, αλλά και αναφορικά με το ποιες κατηγορίες των προσωπικών τους δεδομένων θα περιλαμβάνονται στους καταλόγους αυτούς. Οι πάροχοι από την πλευρά τους οφείλουν να ενημερώνουν τους τελικούς χρήστες για τον σκοπό που θα επιτελεί ο εκάστοτε κατάλογος.

IV.2.5. Οι ανεπιθύμητες απευθείας επικοινωνίες για διαφημιστικούς σκοπούς

Το ζήτημα της προώθησης υπηρεσιών ή/ και προϊόντων μέσω της επικοινωνίας της πωλήτριας εταιρείας απευθείας με τον τελικό χρήστη, ο οποίος λογίζεται ως υποψήφιος πελάτης, έχει λάβει τα τελευταία χρόνια δραματικές διαστάσεις, είτε η προώθηση λαμβάνει χώρα μέσω τηλεφωνικών κλήσεων, γραπτών μηνυμάτων είτε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου.

IV.2.5.1. Το ισχύον νομοθετικό πλαίσιο

Ίσως η σημαντικότερη ρύθμιση που εισήγαγε η υπό κατάργηση οδηγία 2002/58/ΕΚ, είναι αυτή του άρθρου 13, η οποία αφορά τις «*Αυτόκλητες κλήσεις*» και στοχεύει στον περιορισμό, αν όχι στην απαγόρευση, των ανεπιθύμητων εμπορικών επικοινωνιών που δέχονται οι τελικοί χρήστες.

Στην ελληνική έννομη τάξη, μέχρι και σήμερα, το θέμα σχετικά με τις ανεπιθύμητες εμπορικές επικοινωνίες που δέχονται οι τελικοί χρήστες για σκοπούς προώθησης υπηρεσιών/

προϊόντων και εν γένει διαφημιστικούς σκοπούς, ρυθμίζεται σύμφωνα με την ως άνω οδηγία όπως ενσωματώθηκε με το άρθρο 11 Ν. 3471/2006, το οποίο τιτλοφορείται ως: «*Μη ζητηθείσα επικοινωνία*» [122].

Σύμφωνα με την πρώτη παράγραφο του άρθρου 11 Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, η χρήση αυτομάτων συστημάτων κλήσης, ήτοι χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης ή εν γένει διαφημιστικούς σκοπούς, μέσω τηλεμοιοτυπίας ή μέσω ηλεκτρονικού ταχυδρομείου, επιτρέπεται μόνο στην περίπτωση κατά την οποία ο τελικός χρήστης έχει δώσει εκ των προτέρων τη ρητή[123] του συγκατάθεση[124] ως προς αυτό[125]. Το σύστημα αυτό ονομάζεται «opt- in». Η διάταξη αυτή αποτελεί ενσωμάτωση στο ελληνικό δίκαιο της οδηγίας ePrivacy, η οποία απαγορεύει να σταθμιστεί το έννομο συμφέρον

---

[122] Οι παράγραφοι 1 και 2 του εν λόγω άρθρου τροποποιήθηκαν δυνάμει του άρθρου 16 Ν. 3917/2011, οι παράγραφοι 3 και 4 δυνάμει του άρθρου 172 παρ. 1 Ν. 4070/2012, προστέθηκαν οι παράγραφοι 5 και 6 δυνάμει του άρθρου 172 παρ. 2 Ν. 4070/2012, η μέχρι πρότινος παράγραφος 5 αναριθμήθηκε σε παράγραφο 7 δυνάμει της του άρθρου 172 παρ. 3 Ν. 4070/2012 και προστέθηκε η παράγραφος 8 δυνάμει του άρθρου 172 παρ. 4 Ν. 4070/2012. Η σημερινή μορφή του άρθρου άρα έχει ως κατωτέρω: «***1. Η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, (με ή) χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.***
2. Δεν επιτρέπεται η πραγματοποίηση μη ζητηθεισών επικοινωνιών με ανθρώπινη παρέμβαση (κλήσεων) για τους ανωτέρω σκοπούς, εφόσον ο συνδρομητής έχει δηλώσει προς τον φορέα παροχής της διαθέσιμης στο κοινό υπηρεσίας, ότι δεν επιθυμεί γενικώς να δέχεται τέτοιες κλήσεις.
3. Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεση του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων και αυτό κατά τη συλλογή των στοιχείων επαφής, καθώς και σε κάθε μήνυμα, σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση. […]»

[123] Η χρήση της έννοιας «ρητής συγκατάθεσης» έχει χαρακτηριστεί ως «αντιενωσιακή» αφού αντίκειται στο πνεύμα της Οδηγίας ePrivacy, η οποία απαιτεί απλώς να υπάρχει συγκατάθεση χωρίς να είναι απαραίτητα ρητή, βλ. αναλυτικότερα: Ε. Μαργαρίτης «*Προσωπικά Δεδομένα & Προστασία Καταναλωτή*», Νομική Βιβλιοθήκη, 2020, σελ. 73- 75.

[124] Το άρθρο 2 Ν. 3471/2006 παραπέμπει ως προς τον ορισμό της «συγκατάθεσης» στον Ν. 2472/1997, ο οποίος στο άρθρο 2 περ. ια όριζε ως συγκατάθεση του υποκειμένου των δεδομένων «*κάθε ελεύθερη, ρητή και ειδική δήλωση βουλήσεως, που εκφράζεται με τρόπο σαφή και εν πλήρη επιγνώσει, και με την οποία, το υποκείμενο των δεδομένων, αφού προηγουμένως ενημερωθεί, δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν*». Ωστόσο, δεδομένου ότι ο Ν. 2472/1997 έχει καταργηθεί με το άρθρο 84 Ν. 4626/2019, το άρθρο 83 Ν. 4624/2019 ορίζει ότι σε περίπτωση που διατάξεις της κείμενης νομοθεσίας παραπέμπουν στον 2472/1997, η παραπομπή αυτή θα νοείται ως αναφορά στις οικείες διατάξεις του ΓΚΠΔ και του Ν. 4624/2019.

[125] Ε. Μαργαρίτης «*Προσωπικά Δεδομένα & Προστασία Καταναλωτή*», Νομική Βιβλιοθήκη, 2020, σελ. 71.

του υπεύθυνου επεξεργασίας με εκείνο του υποκειμένου των δεδομένων, όταν πρόκειται για εμπορική προώθηση που λαμβάνει χώρα χωρίς την ανθρώπινη παρέμβαση.

Ως μόνη εξαίρεση της «ρητής συγκατάθεσης» της πρώτης παραγράφου του ως άνω άρθρου, εισάγεται με την παράγραφο 3 του ίδιου άρθρου, όπως τροποποιήθηκε και ισχύει, και αφορά στην περίπτωση που ο υπεύθυνος επεξεργασίας έχει λάβει τα στοιχεία του συνδρομητή στο πλαίσιο της πώλησης υπηρεσιών/ προϊόντων ή άλλης συναλλαγής που τυχόν υπήρξε μεταξύ τους και τα χρησιμοποιεί για την απευθείας προώθηση παρόμοιων υπηρεσιών/ προϊόντων και όπως κατά τα λοιπά ορίζεται από την ως άνω παράγραφο. Το σύστημα αυτό ονομάζεται «soft opt- in».

Σύμφωνα με τη δεύτερη παράγραφο του άρθρου 11 Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, οι τηλεφωνικές κλήσεις, οι οποίες πραγματοποιούνται με ανθρώπινη παρέμβαση («cold calls») για διαφημιστικούς σκοπούς, επιτρέπονται γενικά, εκτός εάν ο τελικός χρήστης δηλώσει ρητά ότι δεν επιθυμεί να τις λαμβάνει. Η διάταξη αυτή ενσωμάτωσε στην ελληνική έννομη τάξη το άρθρο 13 § 3 της οδηγίας ePrivacy, ύστερα από την τροποποίησή της από την οδηγία 2009/136/ΕΚ[126], σύμφωνα με την οποία δίδεται η δυνατότητα στον εκάστοτε νομοθέτη κάθε κράτους- μέλους να επιλέξει τις προϋποθέσεις με βάση τις οποίες θα γίνονται οι τηλεφωνικές κλήσεις με ανθρώπινη παρέμβαση προς τους τελικούς χρήστες, είτε σε συνέχεια της προηγούμενης συγκατάθεσης των τελευταίων (σύστημα «opt- in»), είτε με τη δήλωση της αντίρρησής τους (σύστημα «opt- out»[127]). Το σύστημα που επέλεξε ο Έλληνας νομοθέτης εν προκειμένω είναι αυτό του «opt- out»[128].

Εντούτοις, με το θεσμικό πλαίσιο όπως ισχύει σήμερα, δεν φαίνεται να προστατεύονται, τουλάχιστον αποτελεσματικά, οι επιφυείς υπηρεσίες επικοινωνιών και, επομένως, οι επικοινωνίες που πραγματοποιούνται μέσω αυτών για διαφημιστικούς λόγους. Η ΑΠΔΠΧ

---

[126] «*Τα κράτη μέλη λαμβάνουν τα ενδεδειγμένα μέτρα προκειμένου να εξασφαλίζεται, ατελώς, ότι οι αυτόκλητες κλήσεις με σκοπό την απευθείας εμπορική προώθηση, σε άλλες, εκτός των προβλεπομένων στις παραγράφους 1 και 2, περιπτώσεις, δεν επιτρέπονται χωρίς τη συγκατάθεση των ενδιαφερομένων συνδρομητών ή όταν πρόκειται για συνδρομητές οι οποίοι δεν επιθυμούν να λαμβάνουν αυτές τις κλήσεις. Η σχετική επιλογή καθορίζεται από την εθνική νομοθεσία*».

[127] Μέσω του συστήματος «opt- out» το φυσικό ή νομικό πρόσωπο δύναται να απευθύνει αντιρρήσεις, αναφορικά με την επεξεργασία των δεδομένων του, είτε απευθείας στον υπεύθυνο επεξεργασίας, ο οποίος οφείλει να τηρεί αρχείο ειδικών αντιρρήσεων, είτε μέσω εγγραφής του σε ειδικό κατάλογο συνδρομητών του εκάστοτε παρόχου τηλεπικοινωνιακών υπηρεσιών βλ. αναλυτικά: https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/proothisiproiontwn/thlefwnikes_kliseis_proothisi

[128] Ε. Μαργαρίτης «*Προσωπικά Δεδομένα & Προστασία Καταναλωτή*», Νομική Βιβλιοθήκη, 2020, σελ. 77.

έκρινε με τη με αριθμό 66/2018 απόφασή της ότι η εφαρμογή «Viber» δεν αποτελεί υπηρεσία ηλεκτρονικών επικοινωνιών σε δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών, αλλά υπηρεσία της Κοινωνίας της Πληροφορίας, οπότε η νομιμότητα αποστολής προωθητικών μηνυμάτων μέσω αυτής θα πρέπει να γίνεται βάσει των διατάξεων του ΓΚΠΔ. Όπως όμως, ορθά παρατήρησε το ΕΣΠΔ, το απόρρητο των επικοινωνιών απαιτεί ειδικότερη προστασία από αυτή που προσφέρεται από τον ΓΚΠΔ και οι επιφυείς υπηρεσίες δεν καλύπτονται πλέον από την οδηγία 2002/58/ΕΚ[129], συνεπώς, καθίσταται αναγκαία η άμεση υιοθέτηση του υπό μελέτη Κανονισμού.

IV.2.5.2. Το μητρώο του άρθρου 11 Ν. 3471/2006

Από τον ελληνικό νόμο προβλέπεται η δημιουργία ειδικών μητρώων- καταλόγων από κάθε πάροχο, στους οποίους συμπεριλαμβάνονται όσοι έχουν εκφράσει την αντίρρησή τους ως προς τη λήψη κλήσεων για απευθείας εμπορική προώθηση/ διαφήμιση, σύμφωνα με το άρθρο 11 § 2 Ν. 3471/2006. Ο πάροχος υποχρεούται να καταρτίζει τους καταλόγους αυτούς χωρίς τη χρέωση των δηλούντων και να τους θέτει στη διάθεση κάθε ενδιαφερομένου[130], τηρώντας με τον τρόπο αυτό ένα δημόσιο μητρώο, το οποίο επιτελεί έναν δημόσιο σκοπό βαρύνουσας σημασίας. Οι διαφημιζόμενοι οφείλουν να προμηθεύονται επικαιροποιημένα αντίγραφα των μητρώων αυτών από τους παρόχους καθώς και να εξασφαλίζουν ότι διαθέτουν τη δήλωση του εκάστοτε συνδρομητή, πραγματοποιηθείσα εντός 30 ημερών από την πραγματοποίηση της διαφημιστικής ενέργειας.

Είναι εύλογο, ότι εφόσον τα στοιχεία ορισμένου προσώπου ευρίσκονται εντός του ειδικού αυτού μητρώου, το ίδιο πρόσωπο δεν θα πρέπει να λαμβάνει οποιαδήποτε προωθητική κλήση κ.λπ. Εντούτοις, στην πραγματικότητα, ακόμη και άτομα που συμπεριλαμβάνονται σε αυτό, συνεχίζουν ακώλυτα να δέχονται κλήσεις και μηνύματα που έχουν ως σκοπό τη διαφήμιση υπηρεσιών/ προϊόντων [131]. Οι προσβολές όμως στις οποίες προβαίνουν οι διαφημιζόμενοι, είναι το δίχως άλλο, πολλαπλάσιες των καταγγελιών ή/ και των δικαστικών

[129] Ε. Μαργαρίτης, «*GDPR και προώθηση προϊόντων μέσω Viber – Σκέψεις με αφορμή την απόφαση 66/2018 της ΑΠΔΠΧ*», Νομική Βιβλιοθήκη, ΔiΜΕΕ, 2/2019, σελ. 182- 187.

[130] Γ. Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018, σελ. 67.

[131] Βλ. ενδεικτικά την πολύ πρόσφατη απόφαση του Μονομελούς Πρωτοδικείου Αθηνών με αριθμό 227/2022 επί αγωγής συνδρομήτριας για παραβίαση του άρθρου 11 Ν. 3471/2006, σχετικό άρθρο διαθέσιμο εδώ: https://www.lawspot.gr/nomika-nea/hrimatiki-ikanopoiisi-50000-eyro-se-syndromitria-toy-mitrooy-arthroy-11-gia-mi

ενεργειών που υποβάλλονται ή/ και ασκούνται από τους προσβαλλόμενους χρήστες[132], όπως προκύπτει από τις σχετικές αποφάσεις της ΑΠΔΠΧ[133].

[132] Μ. Σκόνδρα, «*Σημείωμα στην ΕιρΑμαρ 129/2019 (Ειδ) – Αζήτητη επικοινωνία για σκοπούς εμπορικής προώθησης και ελάχιστη αποζημίωση του Ν. 3471/2006*», Νομική Βιβλιοθήκη, ΔiΜΕΕ, 3/2019, σελ. 477- 479.
[133] Βλ. ενδεικτικά αποφάσεις της ΑΠΔΠΧ με αριθμούς: 64/2016, 65/2016, 66/2016, 62/2018, 63/2018, 30/2019 και 38/2019.

V. ΟΙ ΔΙΑΤΑΞΕΙΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

V.1. Η δομή του Κανονισμού

Ο υπό μελέτη Κανονισμός, τουλάχιστον στο μέχρι τώρα τελευταίο σχέδιό του, αποτελείται από συνολικά 7 κεφάλαια και 30 άρθρα με σκοπό να ενισχυθεί το ήδη υπάρχον νομοθετικό πλαίσιο για την αποτελεσματική προστασία των επικοινωνιών και του απόρρητου χαρακτήρα τους, των πληροφοριών που βρίσκονται στον τερματικό εξοπλισμό του χρήστη, να οριστούν οι Ανεξάρτητες Αρχές που θα εποπτεύουν την ορθή εφαρμογή του και να οριστούν ρητά τα δικαιώματα των χρηστών και οι ποινές στους παραβάτες. Όλα αυτά, πάντοτε, σε συνάρτηση με τη ραγδαία εξέλιξη της τεχνολογίας, την οποία θα πρέπει ο Κανονισμός να ακολουθήσει και να ανταποκριθεί σε αυτή, κάτι που δυστυχώς δεν κατάφερε να πράξει η οδηγία ePrivacy [134]. Ειδικότερα θα γίνει κατωτέρω μια ανασκόπηση των άρθρων του Κανονισμού, ως έχουν μέχρι στιγμής και ως έγιναν δεκτά από το Ευρωπαϊκό Συμβούλιο.

V.2. Κεφάλαιο πρώτο- Γενικές Διατάξεις

V.2.1. Οι ειδικότερες ρυθμίσεις του πρώτου κεφαλαίου

Το κεφάλαιο αυτό αποτελείται από 5 συνολικά άρθρα τα οποία αφορούν στο αντικείμενο του Κανονισμού, ήτοι τις ειδικότερες περιπτώσεις που πραγματεύεται και σε τι συνίσταται ο σκοπός του (άρθρο 1), στο πεδίο εφαρμογής του (άρθρο 2), στα εδαφικά όρια της εφαρμογής του και τις περιπτώσεις που είναι απαραίτητος ο ορισμός εκπροσώπου (άρθρο 3), στους ορισμούς που εμφανίζονται στον Κανονισμό, τους οποίους ερμηνεύει ώστε να γίνεται όσο πιο κατανοητή η ανάγνωσή του (άρθρο 4), ενώ με το τελευταίο, από 10.02.2021 σχέδιο του Κανονισμού προστέθηκε και η συναίνεση ως άρθρο 4α.

Ειδικότερα, με το άρθρο 1 ορίζεται ρητά ο ρόλος τον οποίο καλείται να επιτελέσει ο υπό μελέτη Κανονισμός, ήτοι να θεσπίσει συγκεκριμένους κανόνες σχετικά με την προστασία των θεμελιωδών δικαιωμάτων αλλά και ελευθεριών των φυσικών προσώπων στο πλαίσιο των υπηρεσιών ηλεκτρονικών επικοινωνιών και την προστασία των προσωπικών τους δεδομένων. Επιπλέον, ορίζεται σε ξεχωριστή παράγραφο[135] η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των νομικών προσώπων, στο ίδιο πλαίσιο, καθώς και η ελεύθερη κυκλοφορία των δεδομένων των ηλεκτρονικών επικοινωνιών εντός της Ένωσης. Τέλος, ρητά ορίζεται, όπως

[134] Βλ. Σκέψη 6 του Σχεδίου 02/2021 του Κανονισμού.
[135] Βλ. άρθρο 1 § 2 του σχεδίου 02/2021 του Κανονισμού.

αναφέρθηκε και ανωτέρω ότι ο Κανονισμός αποτελεί εξειδίκευση και συμπλήρωση του κανονισμού ΓΚΠΔ.

Με το άρθρο υπ' αριθμό 2 σκιαγραφείται το πεδίο εφαρμογής του Κανονισμού αναφέροντας ρητά τόσο τις περιπτώσεις στις οποίες εφαρμόζεται, ήτοι στην επεξεργασία του περιεχομένου και των μεταδεδομένων των ηλεκτρονικών επικοινωνιών, στις πληροφορίες του τερματικού εξοπλισμού του χρήστη, στους καταλόγους που είναι διαθέσιμοι στο κοινό και στις επικοινωνίες που πραγματοποιούνται για διαφημιστικούς σκοπούς[136], όσο και τις περιπτώσεις στις οποίες δεν εφαρμόζεται ο Κανονισμός, όπως είναι οι δραστηριότητες που δεν εμπίπτουν στο πεδίο εφαρμογής του ενωσιακού δικαίου, καθώς και οι περιπτώσεις που αφορούν στην εθνική ασφάλεια και άμυνα[137], οι υπηρεσίες ηλεκτρονικών επικοινωνιών, οι οποίες δεν είναι διαθέσιμες στο κοινό, οι δραστηριότητες των αρμόδιων αρχών που στοχεύουν στη διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινών, τα δεδομένα των επικοινωνιών εφόσον έχουν παραληφθεί από τον τελικό χρήστη τον οποίο αφορούν. Καταλήγοντας, αναφέρεται ότι ο Κανονισμός δεν θίγει τις διατάξεις της Οδηγίας 2000/31/ΕΚ[138], ούτε και τις Οδηγίας 2014/53/ΕΕ[139].

Σύμφωνα με την αιτιολογική σκέψη με αριθμό 12 του Κανονισμού, ο τελευταίος θα πρέπει να εφαρμόζεται και στις υπηρεσίες machine to machine και στις υπηρεσίες του Διαδικτύου των Πραγμάτων, αφού κατά την διενέργεια αυτών μεταφέρονται αυτόματα δεδομένα και πληροφορίες μέσω συσκευών ή εφαρμογών λογισμικού με ελάχιστη ή/ και μηδενική συμμετοχή κάποιου φυσικού προσώπου. Επομένως, είναι εύλογο ότι και αυτού του είδους τα δεδομένα πρέπει να προστατευτούν με σκοπό την ασφάλεια των υπηρεσιών αυτών. Η εφαρμογή, όμως, του Κανονισμού εν προκειμένω θα γίνεται μόνο εφόσον η ανταλλαγή των δεδομένων λαμβάνει χώρα μέσω δημόσιου δικτύου ή υπηρεσίας ηλεκτρονικών επικοινωνιών.

Αντίστοιχα, με την αιτιολογική σκέψη με αριθμό 13 του Κανονισμού, εντοπίζεται η ανάγκη εφαρμογής του και στα ασύρματα δίκτυα (wireless networks), θεωρώντας ότι η δραματική ανάπτυξη τέτοιου είδους δικτύων, τα οποία είναι προσβάσιμα σε απροσδιόριστο

---

136 Βλ. αιτιολογική σκέψη 8 του σχεδίου 02/2021 του Κανονισμού.

137 Βλ. αιτιολογική σκέψη 7α του σχεδίου 02/2021 του Κανονισμού.

138 Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 «*για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά*».

139 Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Απριλίου 2014 «*σχετικά με την εναρμόνιση των κρατών μελών σχετικά με τη διαθεσιμότητα ραδιοεξοπλισμού στην αγορά και την κατάργηση της οδηγίας 1999/5/ΕΚ*».

αριθμό τελικών χρηστών σε δημόσιους ή ημι-ιδιωτικούς χώρους, τοποθετεί τις επικοινωνίες που μεταδίδονται μέσω των δικτύων αυτών σε αρκετά δυσχερή θέση και επομένως θεσπίζεται η προστασία τους.

Σύμφωνα με το άρθρο 3, ο Κανονισμός εφαρμόζεται, από χωρική άποψη, κατά την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών σε τελικούς χρήστες εντός της Ένωσης, κατά την επεξεργασία του περιεχομένου και των μεταδεδομένων της επικοινωνίας των τελικών χρηστών που βρίσκονται εντός της Ένωσης, κατά την προστασία των πληροφοριών στον τερματικό εξοπλισμό των τελικών χρηστών που βρίσκονται εντός της Ένωσης, κατά την παροχή καταλόγων διαθέσιμων στο κοινό τελικών χρηστών που βρίσκονται εντός της Ένωσης και κατά την εκτέλεση επικοινωνιών για διαφημιστικούς λόγους προς τελικούς χρήστες, οι οποίοι βρίσκονται εντός της Ένωσης. Ο Κανονισμός, πάντως, θα πρέπει να εφαρμόζεται ανεξαρτήτως εάν η εν λόγω επεξεργασία πραγματοποιείται εντός της Ένωσης ή εκτός αυτής ή ανεξαρτήτως εάν ο πάροχος ή το πρόσωπο που πραγματοποιεί την εν λόγω επεξεργασία βρίσκεται εντός ή εκτός της Ένωσης[140] και σε αυτή την περίπτωση θα πρέπει να διορίζεται από τον πάροχο εκπρόσωπός του, ο οποίος θα βρίσκεται εγκατεστημένος στην Ένωση, καθώς και να λαμβάνει γνώση αυτού η αρμόδια εποπτική Αρχή. Ο διορισμός αυτός δεν είναι απαραίτητος εφόσον μια τέτοια παροχή έχει περιστασιακό χαρακτήρα και δεν σκοπεύει να θέσει σε κίνδυνο θεμελιώδη δικαιώματα των τελικών χρηστών.

Στο άρθρο 4 εντοπίζονται οι ορισμοί, οι οποίοι θα χρησιμοποιηθούν για την καλύτερη δυνατή κατανόηση του κειμένου του Κανονισμού και την προς ρύθμιση ύλη. Προς διευκόλυνση, ο Κανονισμός παραπέμπει στους ορισμούς του ΓΚΠΔ συνολικά, της οδηγίας 2018/1972, της οδηγίας 2008/63/ΕΚ και της οδηγίας 2015/1535, για συγκεκριμένους ορισμούς, και θέτει και ο ίδιος ο Κανονισμός ορισμούς όπως των δεδομένων ηλεκτρονικής επικοινωνίας, του περιεχομένου της ηλεκτρονικής επικοινωνίας κ.ά.

Στο τελευταίο άρθρο του κεφαλαίου αυτού, το άρθρο 4α, αφορά στη συγκατάθεση, η οποία για τους σκοπούς του παρόντος Κανονισμού ταυτίζεται με αυτή του ΓΚΠΔ, με τη διαφορά ότι οι εν λόγω διατάξεις περί συγκατάθεσης χρήζουν εφαρμογής mutatis mutandis και στα νομικά πρόσωπα. Αφήνεται, όμως, στη διακριτική ευχέρεια των κρατών- μελών να καθορίσουν δια νόμου, τα πρόσωπα τα οποία θα είναι εξουσιοδοτημένα να εκπροσωπούν ένα νομικό

[140] Βλ. αιτιολογική σκέψη με αριθμό 8aaa του σχεδίου 02/2021 του Κανονισμού.

πρόσωπο στην περίπτωση της συγκατάθεσης. Πολλώ δε μάλλον, ορίζεται ότι η συγκατάθεση του τελικού χρήστη θα πρέπει να εφαρμόζεται απευθείας και χωρίς καθυστέρηση. Τέλος, ο τελικός χρήστης που έχει δώσει τη συγκατάθεσή του θα πρέπει να ενημερώνεται ανά τακτά χρονικά διαστήματα σχετικά με τη δυνατότητά του να ανακαλεί την εν λόγω συγκατάθεση.

V.2.2. Οι αλλαγές που επήλθαν στο πρώτο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Στο εναρκτήριο κεφάλαιο του Κανονισμού, όπως διαμορφώθηκε, ύστερα από 3 χρόνια, τον Φεβρουάριο του 2021, εντοπίζονται αρκετές αλλαγές, όπως αναλυτικά εμφαίνεται στον κατωτέρω πίνακα.

Τα δύο σχέδια έχουν διαμορφωθεί ως εξής:

CHAPTER I *GENERAL PROVISIONS*	*CHAPTER I* *GENERAL PROVISIONS*
Article 1 *Subject matter* 1. 1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data. 2. This Regulation ensures free movement of electronic communications data and electronic communications services within the Union, which shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural and legal persons and the protection of natural persons with regard to the processing of personal data. 3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs 1 and 2.	*Article 1* *Subject matter* 1. This Regulation lays down rules regarding the protection of fundamental rights and freedoms of natural ~~and legal persons~~ in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data. **1a. This Regulation lays down rules regarding the protection of the fundamental rights and freedoms of legal persons in the provision and use of the electronic communications services, and in particular their rights to respect of communications.** 2. ~~This Regulation ensures~~ **The** free movement of electronic communications data and electronic communications services within the Union ~~which~~ shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural persons ~~and legal persons~~ and the protection of natural persons with regard to the processing of personal data, **and for protection of communications of legal persons.** 3. The provisions of this Regulation particularise and complement Regulation (EU) 2016/679 by laying down specific rules for the purposes mentioned in paragraphs **1 to 2**.
Article 2 *Material Scope* 1. This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users. 2. This Regulation does not apply to: (a) activities which fall outside the scope of Union law; (b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; (c) electronic communications services which are not publicly available; (d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the	*Article 2* *Material Scope* 1. This Regulation applies to: (a) the processing of electronic communications **content and of electronic communications metadata** carried out in connection with the provision and the use of electronic communications services; (b) **end-users' terminal equipment** information. (c) **the offering of a publicly available directory of end-users of electronic communications services;** (d) **the sending of direct marketing communications to end-users.** 2. This Regulation does not apply to: (a) activities, which fall outside the scope of Union law, **and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out**

safeguarding against and the prevention of threats to public security; 3. The processing of electronic communications data by the Union institutions, bodies, offices and agencies is governed by Regulation (EU) 00/0000 [new Regulation replacing Regulation 45/2001]. 4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC 141 , in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. 5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.	**those activities whether it is a public authority or a private operator acting at the request of a public authority;** (b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; (c) electronic communications services which are not publicly available; (d) activities, **including data processing activities**, of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) **electronic communications data processed after receipt by the end-user concerned**, 4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. 5. This Regulation shall be without prejudice to the provisions of Directive 2014/53/EU.
Article 3 *Territorial scope and representative* 1. This Regulation applies to: (a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required; (b) the use of such services; (c) the protection of information related to the terminal equipment of end-users located in the Union. 2. Where the provider of an electronic communications service is not established in the Union it shall designate in writing a representative in the Union. 3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located. 4. The representative shall have the power to answer questions and provide information in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation. 5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against a natural or legal person who processes electronic communications data in connection with the provision of electronic communications services from outside the Union to end-users in the Union.	*Article 3* *Territorial scope and representative* 1. This Regulation applies to: (a) the provision of electronic communications services to end-users who are in the Union, ~~irrespective of whether a payment of the end-user is required;~~ (aa) **the processing of electronic communications content and of electronic communications metadata of end-users who are in the Union;** ~~(b)~~ (c) the protection of **terminal equipment** information of end-users **who are** in the Union. (cb) **the offering of publicly available directories of end-users of electronic communications services who are in the Union;** (cc) **the sending of direct marketing communications to end-users who are in the Union.** 2. Where the provider of an electronic communications service, **the provider of a publicly available directory, or a person using electronic communications services to send direct marketing communications, or a person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment** is not established in the Union it shall designate in writing, **within one month from the start of its activities**, a representative in the Union **and communicate it to the competent Supervisory Authority.** 2a. **The requirements laid down in paragraph 2 shall not apply if activities listed in paragraph 1 are occasional and are unlikely to result in a risk to the fundamental rights of end-users taking into account the nature, context, scope and purpose of those activities.** 3. The representative shall be established in one of the Member States where the end-users of such electronic communications services are located. 4. **The representative shall be mandated by the provider or person it represents to be addressed in addition to or instead of the provider it represents, in particular, to supervisory authorities, and end-users, on all issues related to processing electronic communications data for the purposes of ensuring compliance with this Regulation.**

141 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1–16).

	5. The designation of a representative pursuant to paragraph 2 shall be without prejudice to legal actions, which could be initiated against **the provider or person it represents.** 6. **This Regulation applies to the processing of personal data by a provider not established in the Union, but in a place where Member State law** ***applies by virtue of public international law.***
Article 4 *Definitions* 1. For the purposes of this Regulation, following definitions shall apply: (a) the definitions in Regulation (EU) 2016/679; (b) the definitions of 'electronic communications network', 'electronic communications service', 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service', 'end-user' and 'call' in points (1), (4), (5), (6), (7), (14) and (21) respectively of Article 2 of [Directive establishing the European Electronic Communications Code]; (c) the definition of 'terminal equipment' in point (1) of Article 1 of Commission Directive 2008/63/EC. 2. For the purposes of point (b) of paragraph 1, the definition of 'interpersonal communications service' shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service. 3. In addition, for the purposes of this Regulation the following definitions shall apply: (a) 'electronic communications data' means electronic communications content and electronic communications metadata; (b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound; (c) 'electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication; (d) 'publicly available directory' means a directory of end-users of electronic communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service; (e) 'electronic mail' means any electronic message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient; (f) 'direct marketing communications' means any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc.; (g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems; (h) 'automated calling and communication systems' means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and	*Article 4* *Definitions* 1. For the purposes of this Regulation, following definitions shall apply: (a) the definitions in Regulation (EU) 2016/679; (b) the definitions of 'electronic communications network', 'electronic communications service', 'interpersonal communications service', 'number-based interpersonal communications service', 'number-independent interpersonal communications service', 'end-user' and 'call' in **paragraphs** (1), (4), (5), (6), (7), (14) and **(31)** respectively of Article 2 of Directive **(EU) 2018/1972**; (c) the definition of 'terminal equipment' in ~~point (1) of~~ Article 1 **(1)** of Commission Directive 2008/63/EC; **(d) the definition of 'information society service' in point (b) of Article 1 (1) of Directive (EU) 2015/1535.** 2. For the purposes **of this Regulation**, the definition of 'interpersonal communications service' **referred to in point (b) of paragraph 1** shall include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service. **2a. For the purposes of this Regulation, the definition of 'processing' referred to in Article 4 (2) of Regulation 2016/679 shall not be limited to processing of personal data.** 3. In addition, for the purposes of this Regulation the following definitions shall apply: (a) 'electronic communications data' means electronic communications content and electronic communications metadata; (b) 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound; (c) 'electronic communications metadata' means data processed **by means of** electronic communications **services** for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication; (d) 'publicly available directory' means a directory of end-users of **number-based interpersonal** communications services, whether in printed or electronic form, which is published or made available to the public or to a section of the public, including by means of a directory enquiry service **and the main function of which is to enable identification of such end-users;** (e) 'electronic **message**' means any ~~electronic~~ message containing information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient, **including e-mail, SMS, MMS and functionally equivalent applications and techniques**; (f) 'direct marketing communications' means any form of advertising, whether written or oral, sent **via a publicly available electronic communications service directly** to one or more **specific** end-users, including **the placing of voice-to- voice calls, the** use of

transmitting sounds which are not live speech, including calls made using automated calling and communication systems which connect the called person to an individual.	automated calling and communication systems with or without human interaction, electronic message etc.; (g) 'direct marketing voice-to-voice calls' means live calls, which do not entail the use of automated calling systems and communication systems; (h) 'automated calling and communication systems' means systems capable of automatically initiating calls to one or more recipients in accordance with instructions set for that system, and transmitting sounds which are not live speech, including calls made using automated calling and communication systems which connect the called person to an individual; **(i) 'direct marketing calls' means direct marketing voice-to-voice calls and calls made via automated calling and communication systems for the purpose of direct marketing.** **(j) 'location data' means data processed by means of an electronic** **communications network or service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;**
-	***Article 4a*** ***Consent*** **1. The provisions for consent provided for under Regulation (EU) 2016/679/EU shall apply to natural persons and, mutatis mutandis, to legal persons.** **1a. Paragraph 1 is without prejudice to national legislation on determining the persons who are authorised to represent a legal person in any dealings with third parties or in legal proceedings.** **2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8 (1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.** **2aa. Consent directly expressed by an end-user in accordance with Paragraph (2) shall prevail over software settings. Any consent requested and given by an end-user to a service shall be directly implemented, without any further delay, by the applications of the end user's terminal, including where the storage of information or the access of information already stored in the end- user's terminal equipment is permitted.** **2a. As far as the provider is not able to identify a data subject, the technical protocol showing that consent was given from the terminal equipment shall be sufficient to demonstrate the consent of the end-user according Article 8 (1) (b).** **3. End-users who have consented to the processing of electronic communications data in accordance with this Regulation shall be reminded of the possibility to withdraw their consent at periodic intervals of [no longer than 12 months], as long as the processing continues, unless the end-user requests not to receive such reminders.**

Πίνακας 1: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Από την παράθεση των δύο σχεδίων, ήτοι της από 01.2017 πρότασης Κανονισμού της Ευρωπαϊκής Επιτροπής και του από 02.2021 σχεδίου, το οποίο έγινε δεκτό από το Ευρωπαϊκό Συμβούλιο, γίνονται δεκτά τα κάτωθι.

Βασικό ζήτημα το οποίο ανέκυψε στη σχέση του Κανονισμού με τον ΓΚΠΔ είναι η επέκταση του Κανονισμού και στα νομικά πρόσωπα, σε αντίθεση με τον δεύτερο κανονισμό. Ως εκ τούτου, ενώ αρχικά υπήρχε μια μικρή αναφορά στην εφαρμογή του Κανονισμού και στα νομικά πρόσωπα, στο τελευταίο σχέδιό του, εντοπίζεται ολόκληρη παράγραφος (βλ. ανωτέρω, Άρθρο 1 § 1α- 2ου Σχεδίου), η οποία κατοχυρώνει την προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών των νομικών προσώπων όσον αφορά στην παροχή και χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών και ειδικότερα των δικαιωμάτων της προστασίας των επικοινωνιών.

Επιπλέον, επεκτείνεται η εφαρμογή του Κανονισμού και στο περιεχόμενο των ηλεκτρονικών επικοινωνιών αλλά και στα μεταδεδομένα τα οποία αυτή φέρει (βλ. Άρθρο 2 § 1, περ. α'- 2ου Σχεδίου), ζήτημα ακανθώδες και αρκετά θολό που πολλάκις έχει απασχολήσει την ελληνική νομολογία, όπως εκτενώς αναφέρθηκε ανωτέρω. Περαιτέρω, επεκτείνεται η εφαρμογή του στις πληροφορίες που βρίσκονται αποθηκευμένες στον τερματικό εξοπλισμό του τελικού χρήστη (βλ. Άρθρο 2 § 1, περ. β'- 2ου σχεδίου), στους καταλόγους που είναι διαθέσιμοι στο κοινό (βλ. Άρθρο 2 § 1, περ. γ'- 2ου σχεδίου) αλλά και στην επικοινωνία με τον τελικό χρήστη για λόγους προώθησης υπηρεσιών/ προϊόντων (βλ. Άρθρο 2 § 1, περ. δ'- 2ου σχεδίου).

Στο τρίτο άρθρο του Κανονισμού εντοπίζονται αρκετές αλλαγές, αφού εντάσσονται και πάλι στην προστασία του απορρήτου τόσο το περιεχόμενο των επικοινωνιών όσο και τα μεταδεδομένα του τελικού χρήστη εντός της Ένωσης (βλ. Άρθρο 3 § 1, περ. αα'- 2ου σχεδίου), οι πληροφορίες στον τερματικό εξοπλισμό του χρήστη εντός της Ένωσης (βλ. Άρθρο 3 § 1, περ. γ'- 2ου σχεδίου), οι κατάλογοι που είναι διαθέσιμοι στο κοινό εντός της Ένωσης (βλ. Άρθρο 3 § 1, περ. γβ'- 2ου σχεδίου) και η επικοινωνία με τον τελικό χρήστη για διαφημιστικούς σκοπούς εντός της Ένωσης (βλ. Άρθρο 3 § 1, περ. γγ'- 2ου σχεδίου) αλλά προστίθενται και διατάξεις σχετικές με τον ορισμό εκπροσώπου σε περίπτωση που ο πάροχος υπηρεσίας ηλεκτρονικών επικοινωνιών, ο πάροχος των καταλόγων ή το πρόσωπο που κάνει χρήση της τηλεφωνικής επικοινωνίας για λόγους προώθησης υπηρεσιών/ προϊόντων δεν είναι εγκατεστημένος στην Ένωση (βλ. Άρθρο 3 § 2 επ.).

Στο άρθρο 4 του δεύτερου πρόσφατου σχεδίου, όπως παρατίθεται κατωτέρω, εντοπίζεται μια σημαντικότατη αλλαγή. Στον ορισμό του ηλεκτρονικού μηνύματος το από 02/2021 σχέδιο του Κανονισμού, σε αντίθεση με την αρχική πρόταση της Επιτροπής, εντάσσει και τα ηλεκτρονικά μηνύματα (e-mail), SMS, MMS και τις λειτουργικά ισοδύναμες εφαρμογές

και τεχνικές (βλ. Άρθρο 4 § 3, περ. ε). Η αλλαγή αυτή είναι εξαιρετικά σημαντική και ο λόγος για τον οποίο έγινε είναι προφανώς διότι το έτος 2017 η χρήση των ηλεκτρονικών επικοινωνιών μέσω, για παράδειγμα, των εφαρμογών «Messenger» και «Viber», δεν ήταν τόσο εκτεταμένη όσο κατά το έτος 2021[142].

V.3. Κεφάλαιο δεύτερο- Προστασία των ηλεκτρονικών επικοινωνιών των τελικών χρηστών και των πληροφοριών που είναι αποθηκευμένες στον τερματικό τους εξοπλισμό

V.3.1. Οι ειδικότερες ρυθμίσεις του δεύτερου κεφαλαίου

Το δεύτερο κεφάλαιο αποτελείται από 8 άρθρα τα οποία πραγματεύονται το απόρρητο των δεδομένων των ηλεκτρονικών επικοινωνιών (άρθρο 5), τις περιπτώσεις κατά τις οποίες μπορεί να είναι επιτρεπτή η επεξεργασία των δεδομένων ηλεκτρονικών επικοινωνιών (άρθρο 6), τις περιπτώσεις που δύναται να είναι επιτρεπτή η επεξεργασία του περιεχομένου των ηλεκτρονικών επικοινωνιών (άρθρο 6α), τις περιπτώσεις κατά τις οποίες είναι επιτρεπτή η επεξεργασία των μεταδεδομένων των ηλεκτρονικών επικοινωνιών (άρθρο 6β), τις περιπτώσεις κατά τις οποίες υπάρχει σύμφωνη επεξεργασία των μεταδεδομένων των ηλεκτρονικών επικοινωνιών (άρθρο 6γ), τι περιπτώσεις που δύναται να γίνει αποθήκευση αλλά και επιβάλλεται η διαγραφή των δεδομένων των ηλεκτρονικών επικοινωνιών (άρθρο 7), ορίζεται η προστασία των πληροφοριών των πληροφοριών που βρίσκονται στον τερματικό εξοπλισμό του χρήστη (άρθρο 8) και τέλος. ορίζονται οι περιορισμοί στους οποίους υπόκεινται τα άρθρα 5- 8 (άρθρο 11).

Αρχικά, με το άρθρο 5 προστατεύεται οποιοδήποτε δεδομένο ηλεκτρονικών επικοινωνιών (όπως αναφέρθηκε ανωτέρω, σύμφωνα με τον ορισμό που δίδει ο ίδιος ο Κανονισμός, τα δεδομένα απαρτίζονται και από το περιεχόμενο αλλά και από τα μεταδεδομένα της επικοινωνίας) και απαγορεύεται ρητά οποιαδήποτε παραβίαση από οποιονδήποτε των δεδομένων αυτών, συμπεριλαμβανομένης της ακρόασης, της υποκλοπής, της αποθήκευσης κ.λπ. Οι τρόποι με τους οποίους μια τέτοια παραβίαση μπορεί να πραγματοποιηθεί, λόγω της διαρκούς εξέλιξης της τεχνολογίας, συνεχώς πληθαίνουν. Η

[142] Βλ. Δελτίου Τύπου ΕΛ.ΣΤΑΤ. του έτους 2021, από όπου εμφαίνεται η ραγδαία αύξηση του ποσοστού πρόσβασης στο διαδίκτυο (σελ. 1- 2) αλλά και του ποσοστού πραγματοποίησης τηλεφωνικών κλήσεων ή/ και βιντεοκλήσεων μέσω τέτοιου είδους εφαρμογών (σελ. 3) https://www.statistics.gr/documents/20181/bfeda5cf-6bce-2b1d-5027-8983222da4d6

παραβίαση δε αυτή, σύμφωνα με την αιτιολογική σκέψη με αριθμό 15, μπορεί να λαμβάνει χώρα είτε με ανθρώπινη παρέμβαση, είτε αυτοματοποιημένα.

Με το άρθρο 6 ορίζονται περιοριστικά οι 4 περιπτώσεις κατά τις οποίες καθίσταται επιτρεπτή η επεξεργασία των δεδομένων των ηλεκτρονικών επικοινωνιών από τους παρόχους. Έτσι είναι δυνατό οι πάροχοι να προχωρήσουν στην επεξεργασία αυτή, εφόσον η επεξεργασία είναι απαραίτητη για την παροχή της εν λόγω υπηρεσίας ηλεκτρονικών επικοινωνιών, για την ασφάλεια των υπηρεσιών και των δικτύων των ηλεκτρονικών επικοινωνιών ή για να εντοπιστούν τεχνικά σφάλματα, επιθέσεις κ.λπ., για την προστασία από τους κινδύνους και τις επιθέσεις στον τερματικό εξοπλισμό των χρηστών και για τη συμμόρφωση του παρόχου με τις νομικές υποχρεώσεις του. Σε κάθε δε περίπτωση, θα πρέπει η επεξεργασία να λαμβάνει χώρα αποκλειστικά για το χρονικό διάστημα για το οποίο είναι απαραίτητο, ώστε να επιτευχθεί ο απαιτούμενος σκοπός. Οι πάροχοι πάντως και σε κάθε περίπτωση είναι υποχρεωμένοι να διασφαλίζουν το απόρρητο των δεδομένων των ηλεκτρονικών επικοινωνιών εισάγοντας μέτρα ασφαλείας σύμφωνα με το άρθρο 40 της οδηγίας 2018/1972 και με το άρθρο 32 του κανονισμού 2016/679[143].

Αντίστοιχα, το άρθρο 6α προβλέπει τις 2 περιπτώσεις κατά τις οποίες είναι επιτρεπτή η επεξεργασία του περιεχομένου των ηλεκτρονικών επικοινωνιών, οι οποίες βασίζονται κατ' αρχήν στη συγκατάθεση του τελικού χρήστη της υπηρεσίας. Η πρώτη καθιστά επιτρεπτή την επεξεργασία του περιεχομένου των επικοινωνιών του, εφόσον ο τελικός χρήστης έχει δώσει τη συγκατάθεσή του ως προς αυτό, για τον σκοπό της παροχής μιας υπηρεσίας, που ο ίδιος αιτήθηκε, με την επιφύλαξη της μη ζημίας ή έστω προσβολής θεμελιωδών δικαιωμάτων τρίτου προσώπου. Η επεξεργασία αυτή καθίσταται επίσης επιτρεπτή σε περίπτωση που όλοι οι εμπλεκόμενοι τελικοί χρήστης έχουν δώσει τη συγκατάθεσή του ως προς αυτό. Προβλέπεται δε στη δεύτερη περίπτωση, η εκπόνηση εκτίμησης αντικτύπου από την πλευρά του παρόχου.

Το άρθρο 6β προβλέπει τις 6 περιπτώσεις, που όταν συντρέχουν καθίσταται επιτρεπτή η επεξεργασία των μεταδεδομένων των επικοινωνιών. Ως εκ τούτου, για τη σύννομη επεξεργασία των μεταδεδομένων της ηλεκτρονικής επικοινωνίας, θα πρέπει είτε η επεξεργασία να είναι απαραίτητη για σκοπούς διαχείρισης ή βελτιοποίησης του δικτύου, είτε να είναι απαραίτητη για την εκτέλεση μιας σύμβασης παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, είτε ο τελικός χρήστης να έχει δώσει τη συγκατάθεσή του, είτε είναι απαραίτητη

[143] Βλ. αιτιολογική σκέψη 15αα του σχεδίου 02/2021 του Κανονισμού.

για την προστασία ζωτικού συμφέροντος φυσικού προσώπου. Ακόμη, ορίζεται ότι δύναται να πραγματοποιηθεί επεξεργασία σε δεδομένα θέσης για επιστημονικούς ή ιστορικούς λόγους εφόσον όμως αυτά ψευδονυμοποιηθούν [144] ή η επεξεργασία τους δεν ήταν δυνατή με πληροφορίες που καθίστανται ανώνυμες και δεδομένα τοποθεσίας τα οποία διαγράφονται ή τα υπό επεξεργασία δεδομένα θέσης δεν θα χρησιμοποιηθούν για τη δημιουργία προφίλ του χρήστη. Τέλος, η επεξεργασία μεταδεδομένων διάφορων των δεδομένων θέσης, μπορεί να πραγματοποιηθεί για επιστημονικούς, ιστορικούς ή στατιστικούς λόγους, υπό την προϋπόθεση ότι η επεξεργασία θα λάβει χώρα σύμφωνα με το ενωσιακό και εγχώριο νομικό πλαίσιο και θα τηρηθούν όλα τα απαραίτητα μέτρα. Το άρθρο αυτό καταλήγει στην υποχρέωση του παρόχου να μην καθιστά γνωστά σε τρίτους τέτοιου είδους μεταδεδομένα, εκτός εάν έχουν καταστεί ανώνυμα.

Από τη σύγκριση των άρθρων με αριθμό 6α και 6β, γίνεται αντιληπτό ότι η προστασία των μεταδεδομένων της επικοινωνίας έχει περισσότερες πιθανότητες να «αρθεί» σε σχέση με την προστασία του περιεχομένου της επικοινωνίας, πάντοτε βέβαια με την επιφύλαξη του άρθρου 6.

Με το άρθρο 6γ εισάγεται η υποχρέωση του παρόχου, σε περίπτωση που η επεξεργασία των προηγούμενων άρθρων δεν βασίζεται στη συγκατάθεση του τελικού χρήστη ή σε ειδικότερο νόμο, να λαμβάνει υπόψη του ορισμένες παραμέτρους προκειμένου να εξακριβώνει εάν η εν λόγω επεξεργασία των μεταδεδομένων πραγματοποιείται για τον σκοπό για τον οποίο αρχικά συλλέχθηκαν. Τέτοιες παράμετροι είναι ενδεικτικά, οποιαδήποτε σύνδεση μεταξύ των σκοπών επεξεργασίας και των λόγων που καθιστούν απαραίτητη την περαιτέρω επεξεργασία, το πλαίσιο εντός του οποίου συλλέχθησαν τα δεδομένα αυτά, κ.ά. Εν συνεχεία, προβλέπονται οι περιπτώσεις που μια τέτοια επεξεργασία μπορεί να πραγματοποιηθεί, εφόσον θεωρηθεί σύννομη, και είναι η περίπτωση κατά την οποία η επεξεργασία δεν ήταν δυνατό να πραγματοποιηθεί με την επεξεργασία πληροφοριών που ανωνυμοποιήθηκαν και μεταδεδομένων που διαγράφηκαν, η περίπτωση που η επεξεργασία περιορίζεται αποκλειστικά σε ψευδονυμοποιημένα μεταδεδομένα και η περίπτωση που δεν δημιουργείται προφίλ στον τελικό χρήστη. Εισάγεται και σε αυτό το άρθρο την υποχρέωση του παρόχου να μην καθιστά γνωστά σε τρίτους τέτοιου είδους μεταδεδομένα, εκτός εάν έχουν καταστεί ανώνυμα.

[144] Ως ψευδονυμοποίηση ορίζεται η επεξεργασία των προσωπικών δεδομένων, εν προκειμένω των μεταδεδομένων του τελικού χρήστη, έτσι ώστε να μην είναι πλέον δυνατό να αποδοθούν σε συγκεκριμένο φυσικό πρόσωπο χωρίς να είναι απαραίτητη η χρήση συμπληρωματικών πληροφοριών.

Με το άρθρο 7 προβλέπεται η διαγραφή των δεδομένων και μεταδεδομένων της επικοινωνίας, εφόσον πλέον δεν είναι απαραίτητα για τον σκοπό για τον οποίο εξ αρχής συλλέχθηκαν. Όσον αφορά στα μεταδεδομένα, ο Κανονισμός θέτει την επιφύλαξη των προηγούμενων άρθρων ως προς τη διαγραφή τους. Σε αμφότερες δε τις περιπτώσεις ο Κανονισμός εισάγει την έννοια της ανωνυμοποίησης[145].

Με το άρθρο 8 εισάγονται οι τρόποι προστασίας των πληροφοριών που βρίσκονται στον τερματικό εξοπλισμό του χρήστη. Το εν λόγω άρθρο αποτελεί το πιο μακροσκελές άρθρο στο σύνολο του Κανονισμού, αφού καταλαμβάνει σχεδόν 5 σελίδες. Κατ' αρχάς, προβλέπεται η απαγόρευση της επεξεργασία και αποθήκευσης του τερματικού εξοπλισμού του χρήστη πέραν αρκετών, ομολογουμένως, εξαιρέσεων που προβλέπονται περιοριστικά. Συνακόλουθα η επεξεργασία αυτή επιτρέπεται, ενδεικτικά, εάν η επεξεργασία είναι απαραίτητη για την παροχή της υπηρεσίας ηλεκτρονικών επικοινωνιών, εάν ο τελικός χρήστης έχει δώσει τη συγκατάθεσή του, εάν είναι απαραίτητη για την παροχή υπηρεσίας που ο ίδιος ο τελικός χρήστης αιτήθηκε από τον πάροχο, εάν είναι απαραίτητη για την αναβάθμιση λογισμικού κ.ά.

Φτάνοντας στο άρθρο 11, δεδομένου ότι τα άρθρα 9 και 10 έχουν διαγραφεί, εντοπίζονται οι περιορισμοί που πιθανό να τίθενται από την Ένωση ή τα κράτη- μέλη σε σχέση με τα δικαιώματα και τις υποχρεώσεις των άρθρων 5- 8, όπως αναφέρθηκαν και ανωτέρω, υπό τη ρητή προϋπόθεση ότι οι περιορισμοί αυτοί σέβονται απολύτως τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία.

V.3.2. Οι αλλαγές που επήλθαν στο δεύτερο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Στο κεφάλαιο 2 του Κανονισμού εντοπίζονται σημαντικότατες ρυθμίσεις, όπως αναφέρθηκε και ανωτέρω και συνακόλουθα έχει υποπέσει σε αρκετές τροποποιήσεις και κυρίως προσθήκες σε σχέση με την πρόταση της Επιτροπής του έτους 2017. Αυτό γίνεται αντιληπτό ήδη από τον τίτλο του κεφαλαίου, όπου στο μεν σχέδιο του 2017 αναφέρεται η προστασία των ηλεκτρονικών επικοινωνιών που πραγματοποιούνται από φυσικά και νομικά πρόσωπα και των πληροφοριών που βρίσκονται αποθηκευμένες στον τερματικό εξοπλισμό

[145] Ως ανωνυμοποίηση ορίζεται η επεξεργασία των προσωπικών δεδομένων, εν προκειμένω των μεταδεδομένων του τελικού χρήστη, έτσι ώστε να μην είναι πλέον δυνατό να αποδοθούν σε ένα πρόσωπο με την κατάργηση ή τροποποίηση οποιωνδήποτε στοιχείων προσωπικής ταυτοποίησης.

των προσώπων αυτών, ενώ στο σχέδιο του 2021 η προστασία καταλαμβάνει την προστασία των επικοινωνιών των τελικών χρηστών και την ακεραιότητα του τερματικού τους εξοπλισμού.

Ειδικότερα, στα δύο σχέδια εντοπίζονται τα ακόλουθα:

CHAPTER II *PROTECTION OF ELECTRONIC COMMUNICATIONS OF NATURAL AND LEGAL PERSONS AND OF INFORMATION STORED IN THEIR TERMINAL EQUIPMENT*	*CHAPTER II* *PROTECTION OF ELECTRONIC COMMUNICATIONS OF **END-USERS** AND OF **THE INTEGRITY OF** THEIR TERMINAL EQUIPMENT*
Article 5 *Confidentiality of electronic communications data* Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.	Article 5 *Confidentiality of electronic communications data* Electronic communications data shall be confidential. Any interference with electronic communications data, **including** listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance **and** processing of electronic communications data, by **anyone** other than the end-users **concerned**, shall be prohibited, except when permitted by this Regulation.
Article 6 *Permitted processing of electronic communications data* 1. Providers of electronic communications networks and services may process electronic communications data if: (a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose. 2. Providers of electronic communications services may process electronic communications metadata if: (a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120146 for the duration necessary for that purpose; or (b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or (c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous. 3. Providers of the electronic communications services may process electronic communications content only: (a) for the sole purpose of the provision of a specific service to an end-user, if the end-user or end-users concerned have given their consent to the processing of his or her electronic communications content and the provision of that service cannot be fulfilled without the processing of such content; or (b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority. Points (2) and (3) of Article	Article 6 *Permitted processing of electronic communications data* 1. Providers of electronic communications networks and services **shall be permitted to** process electronic communications data **only** if: (a) it is necessary **to provide an electronic communication service;** or (b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults, ~~and/or~~ errors, **security risks or attacks on** electronic communications **networks and services;** **(c) it is necessary to detect or prevent security risks or attacks on end-users' terminal equipment;** **(d) it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security.** **2. Electronic communications data shall only be permitted to be processed for the duration necessary for the specified purpose or purposes according to Articles 6 to 6c and if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous.** **3. A third party acting on behalf of a provider of electronic communications network or services may be permitted to process electronic communications data in accordance with Articles 6 to 6c provided that the conditions laid down in Article 28 of Regulation (EU) 2016/679 are met.**

146 Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (OJ L 310, 26.11.2015, p. 1–18).

36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.	
-	**Article 6a [previous art. 6(3)]** *Permitted processing of electronic communications content* **1. Without prejudice to Article (6) 1, providers of the electronic communications networks and services shall be permitted to process electronic communications content only:** **(a) for the purpose of the provision of a service requested by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned; or** **(b) if all end-users concerned have given their consent to the processing of their electronic communications content for one or more specified purposes.** **2. Prior to the processing in accordance with point (b) of paragraph 1 the provider shall carry out a data protection impact assessment of the impact of the envisaged processing operations on the protection of electronic communications data and consult the supervisory authority if necessary pursuant to Article 36 (1) of Regulation (EU) 2016/679. Article 36 (2) and (3) of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.**
-	**Article 6b [previous art 6(2)]** *Permitted processing of electronic communications metadata* **1. Without prejudice to Article (6) 1, providers of electronic communications networks and services shall be permitted to process electronic communications metadata only if:** **(a) it is necessary for the purposes of network management or network optimisation, or to meet technical quality of service requirements pursuant to Directive (EU) 2018/1972 or Regulation (EU) 2015/212020; or** **(b) it is necessary for the performance of an electronic communications service contract to which the end-user is party, or if necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or** **(c) the end-user concerned has given consent to the processing of communications metadata for one or more specified purposes; or** **(d) it is necessary in order to protect the vital interest of a natural person; or** **(e) in relation to metadata that constitute location data, it is necessary for scientific or historical research purposes or statistical purposes, provided that:** **i. such data is pseudonymised;** **ii. the processing could not be carried out by processing information that is made anonymous, and the location data is erased or made anonymous when it is no longer needed to fulfil the purpose; and** **iii. the location data is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.** **(f) in relation to metadata other than location data, it is necessary for scientific or historical research purposes or statistical purposes, provided that such processing is in accordance with Union or Member State law and subject to appropriate safeguards, including encryption and pseudonymisation, to protect fundamental rights and the interest of the end-users and is in accordance with paragraph**

	6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679. **2a. Data processed under point e and f of paragraph 1 of this article may also be used for the development, production and dissemination of official national and European statistics to the extent necessary for this purpose and in accordance, respectively, with national or Union law.** **2. Without prejudice to Article 6 (3), electronic communications metadata processed pursuant to paragraph 1 (e) shall not be shared by the provider with any third party unless it has been made anonymous.**
-	**Article 6c [Previous art 6(2a)]** *Compatible processing of electronic communications metadata* **1. Where the processing for a purpose other than that for which the electronic communications metadata have been collected under paragraph 1 of Articles 6 and 6b is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11, the provider of electronic communications networks and services shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications metadata are initially collected, take into account, inter alia:** **(a) any link between the purposes for which the electronic communications metadata have been collected and the purposes of the intended further processing;** **(b) the context in which the electronic communications metadata have been collected, in particular regarding the relationship between end-users concerned and the provider;** **(c) the nature of the electronic communications metadata as well as the modalities of the intended further processing, in particular where such data or the intended further processing could reveal categories of data, pursuant to Articles 9 or 10 of Regulation (EU) 2016/679;** **(d) the possible consequences of the intended further processing for end-users;** **(e) the existence of appropriate safeguards, such as encryption and pseudonymisation.** **2. Such processing, if considered compatible, may only take place, provided that:** **(a) the processing could not be carried out by processing information that is made anonymous, and electronic communications metadata is erased or made anonymous as soon as it is no longer needed to fulfil the purpose, and** **(b) the processing is limited to electronic communications metadata that is pseudonymised, and** **(c) the electronic communications metadata is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user, which produces legal effects concerning him or her or similarly significantly affects him or her.** **3. For the purposes of paragraph 1 of this Article, the providers of electronic communications networks and services shall not, without prejudice to Article 6 (3), share such data with any third parties, unless it is made anonymous.**
	~~**Article 6d**~~[147]

[147] Στις 18.09.2019 το Συμβούλιο έθεσε ως επιλογή, ώστε να θεσμοθετηθεί η επεξεργασία δεδομένων ηλεκτρονικών επικοινωνιών με σκοπό τον εντοπισμό, τη διαγραφή και την αναφορά υλικού παιδικής

	~~**Processing of electronic communications data for the purpose of preventing child sexual abuse**~~
Article 7 *Storage and erasure of electronic communications data* 1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679. 2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication. 3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law.	Article 7 *Storage and erasure of electronic communications data* **1. The provider of the electronic communications service shall erase electronic communications content or make that data anonymous when it is no longer necessary for the purpose of processing in accordance to article 6 (1) and 6a (1).** 2. Without prejudice to points (b), **(c) and (d)** of Article 6(1), points (c), **(d), (e), (f), point (g) of Article 6b, Article 6c and points (b) to (g) of Article 8 (1)** the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose **of providing an electronic communication service.** 3. Where the processing of electronic communications metadata takes place for the purpose of billing in accordance with point (b) of Article **6b (1),** the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged, or a payment may be pursued in accordance with national law. **4. Union or Member state law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists.**
Article 8 *Protection of information stored in and related to end-users' terminal equipment* 1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or	Article 8 *Protection of* ***end-users' terminal equipment information*** 1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, ~~including about its software and~~ hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose **of providing an electronic communication service;** or (b) the end-user has given ~~his or her~~ consent; or (c) it is **strictly** necessary for providing ~~an information society~~ **a** service **specifically** requested by the end-user; or (d) if it is necessary **for the sole purpose of audience measuring,** provided that such measurement is carried out by the provider

πορνογραφίας, την προσθήκη του άρθρου 6δ, το οποίο και παρέθεσε αυτούσιο κατά την πρότασή του αυτή (βλ. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_12293_2019_INIT). Σε συνέχεια της πρότασης αυτής, στις 04.10.2019 δημοσιεύθηκε το σχέδιο του τροποποιημένου σχεδίου του Κανονισμού, συμπεριλαμβανομένου του άρθρου 6δ με τίτλο: «*Processing of electronic communications data for the purpose of detecting, deleting and reporting material constituting child pornography*» (βλ. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_12633_2019_INIT). Με το σχέδιο, το οποίο δημοσιεύθηκε στις 08.11.2019, ο τίτλος του άρθρου τροποποιήθηκε ως εξής: «*Processing of electronic communications data for the purpose of preventing child sexual abuse*» (βλ. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_13808_2019_INIT). Με το σχέδιο, το οποίο δημοσιεύθηκε στις 04.11.2020 το άρθρο 6δ διεγράφη εντελώς (βλ. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil%3AST_9931_2020_INIT) και, όπως εμφαίνεται από το τελικό σχέδιο του 02/2021, δεν επανήλθε ποτέ.

(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user. 2. The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if: (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or (b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection. The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied. 3. The information to be provided pursuant to point (b) of paragraph 2 may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner. 4. The Commission shall be empowered to adopt delegated acts in accordance with Article 27 determining the information to be presented by the standardized icon and the procedures for providing standardized icons.	**of the service requested by the end-user, or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested provided that, where applicable, the conditions laid down in Articles 26 or 28 of Regulation (EU) 2016/679 are met; or** **(da) it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud or prevent or detect technical faults for the duration necessary for that purpose; or** **(e) it is necessary for a software update provided that:** **(i) such update is necessary for security reasons and does not in any way change the privacy settings chosen by the end-user,** **(ii) the end-user is informed in advance each time an update is being installed, and** **(iii) the end-user is given the possibility to postpone or turn off the automatic installation of these updates; or** **(f) it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3).** **(g) where the processing for purpose other than that for which the information has been collected under this paragraph is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:** **(i) any link between the purposes for which the processing and storage capabilities have been used or the information have been collected and the purposes of the intended further processing;** **(ii) the context in which the processing and storage capabilities have been used or the information have been collected, in particular regarding the relationship between end-users concerned and the provider;** **(iii) the nature the processing and storage capabilities or of the collecting of information as well as the modalities of the intended further processing, in particular where such intended further processing could reveal categories of data, pursuant to Article 9 or 10 of Regulation (EU) 2016/679;** **(iv) the possible consequences of the intended further processing for end-users;** **(v) the existence of appropriate safeguards, such as encryption and pseudonymisation.** **(h) Such further processing in accordance with paragraph 1 (g), if considered compatible, may only take place, provided that:** **(i) the information is erased or made anonymous as soon as it is no longer needed to fulfil the purpose,** **(ii) the processing is limited to information that is pseudonymised, and** **(iii) the information is not used to determine the nature or characteristics of an end-user or to build a profile of an end-user.** **(i) For the purposes of paragraph 1 (g) and (h), data shall not be shared with any third parties unless the conditions laid down in Article 28 of Regulation (EU) 2016/697 are met, or data is made anonymous.**

	2. The collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment shall be prohibited, except **on the following grounds:** (a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing **or maintaining** a connection; or **(b) the end-user has given consent; or** **(c) it is necessary for the purpose of statistical purposes that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose,** **(d) it is necessary for providing a service requested by the end-user.** **2a. For the purpose of paragraph 2 points (b) and (c), a clear and prominent notice is shall be displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection.** **2b. For the purpose of paragraph 2 points (b) and (c), the collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied.** 3. The information to be provided pursuant **to paragraph 2a** may be provided in combination with standardized icons in order to give a meaningful overview of the collection in an easily visible, intelligible and clearly legible manner. The Commision shall be empowered to adopt delegated acts in accordance with Article **25** determining the information to be presented by the standardized icon and the procedures for providing standardized icons.
Article 9 *Consent* 1. The definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply. 2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet. 3. End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues.	~~Article 9~~
Article 10 *Information and options for privacy settings to be provided* 1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment. 2. Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.	~~Article 10~~

3. In the case of software which has already been installed on 25 May 2018, the requirements under paragraphs 1 and 2 shall be complied with at the time of the first update of the software, but no later than 25 August 2018.	
Article 11 *Restrictions* 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. 2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.	Article 11 *Restrictions* 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1) **(c)** to (e), **(i)** and **(j)** of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. **1a. Article 23 (2) of Regulation (EU) 2016/679 shall apply to any legislative measures referred to in paragraph 1.** 2. Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response.

Πίνακας 2: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Αξιοσημείωτο είναι, ύστερα από τη συγκριτική επισκόπηση του κεφαλαίου και στα δύο ως άνω σχέδια, ότι εντοπίζονται πολλές νέες παράγραφοι στα ήδη υπάρχοντα άρθρα αλλά και ολόκληρα νέα άρθρα, τα οποία δεν υπήρχαν στο πρώτο σχέδιο του Κανονισμού.

Ειδικότερα, προστέθηκαν στο άρθρο 6 δύο επιπλέον λόγοι για τους οποίους οι πάροχοι δύνανται να προχωρούν στην επεξεργασία των δεδομένων της επικοινωνίας (βλ. Άρθρο 6 § 1, περ. γ και δ- 2ου Σχεδίου) και με τα καινούργια άρθρα με αριθμούς 6α, 6β και 6γ, γίνεται αναφορά σε δύο σημαντικότατες έννοιες, αυτή του περιεχομένου της ηλεκτρονικής επικοινωνίας και αυτή των μεταδεδομένων, για τις οποίες δεν υπήρχε πρόβλεψη αρχικά και ορίζεται η σύννομη επεξεργασία τους από τους παρόχους. Στην πρόσφατη τροποποίηση του Κανονισμού βλέπουμε, ακόμη, αρκετά ενισχυμένο το άρθρο 8 που αφορά στην προστασία των πληροφοριών που βρίσκονται αποθηκευμένες στον τερματικό εξοπλισμό των τελικών χρηστών, στο οποίο προστέθηκαν πολλές περιπτώσεις που καθιστούν σύννομη την επεξεργασία των πληροφοριών που βρίσκονται σε αυτόν (βλ. Άρθρο 8 § 1, περ. δ επ.- 2ου Σχεδίου).

Γενικότερα, το κεφάλαιο αυτό του Κανονισμού, φαίνεται να έκανε βήματα προς την αυστηροποίηση των ήδη υπάρχοντων κανόνων και στην επέκταση του πλαισίου προστασίας. Όμως, εντοπίζεται και η απώλεια δύο άρθρων, του άρθρου 9 και του άρθρου 10.

V.4. Κεφάλαιο τρίτο- Το δικαίωμα των τελικών χρηστών στον έλεγχο των ηλεκτρονικών τους επικοινωνιών

V.4.1. Οι ειδικότερες ρυθμίσεις του τρίτου κεφαλαίου

Το συγκεκριμένο κεφάλαιο ασχολείται με την ένδειξη ταυτότητας και τον περιορισμό της αναγνώρισης της καλούσας και συνδεδεμένης γραμμής (άρθρο 12), με τις εξαιρέσεις αναφορικά με την ένδειξη της ταυτότητας και με τον περιορισμό της αναγνώρισης καλούσας και συνδεδεμένης γραμμής (άρθρο 13), με τη φραγή ανεπιθύμητων, κακόβουλων και ενοχλητικών κλήσεων (άρθρο 14), με τους καταλόγους οι οποίοι βρίσκονται στη διάθεση του κοινού (άρθρο 15) και με τις ανεπιθύμητες και άμεσες επικοινωνίες που αφορούν διαφημιστικούς σκοπούς (άρθρο 16).

Το άρθρο 12 ορίζει τη δυνατότητα του καλούντα τελικού χρήστη να αιτείται από τον πάροχο των επικοινωνιών να μην εμφαίνεται η ταυτότητα της καλούσας γραμμής του ανά κλήση, σύνδεση ή/ και μόνιμα και στον καλούμενο τελικό χρήστη να μην εμφαίνεται η ταυτότητα της καλούσας γραμμής στις εισερχόμενες κλήσεις, να απορρίπτει εισερχόμενες κλήσεις όταν δεν εμφαίνεται η ταυτότητα του καλούντος και να εξαλείφει ο ίδιος την ένδειξη ταυτότητάς της συνδεδεμένης γραμμής στον καλούντα τελικό χρήστη. Όλες οι ανωτέρω δυνατότητες, κατά την παράγραφο 2 του ίδιου άρθρου θα πρέπει να παρέχονται δωρεάν στους τελικούς χρήστες και με απλά μέσα.

Με το άρθρο 13 προβλέπονται οι εξαιρέσεις και οι περιορισμοί αναφορικά με τα δικαιώματα των τελικών χρηστών, όπως θεσπίστηκαν από το άρθρο 12, ήτοι εφόσον πραγματοποιείται μια κλήση έκτακτης ανάγκης, ακόμη και αν ο τελικός χρήστης έκανε χρήση της δυνατότητας μη εμφάνισης της ταυτότητας της καλούσας γραμμής, ο πάροχος, παρά την επιλογή αυτή του χρήστη, την προσωρινή του άρνηση ή την έλλειψη συγκατάθεσής του για την επεξεργασία των μεταδεδομένων της επικοινωνίας, δύναται να εμφανίσει την ταυτότητα αυτή στους οργανισμούς που ασχολούνται με επικοινωνίες έκτακτης ανάγκης. Επίσης, κατά την παράγραφο 1α του ίδιου άρθρου, εάν ο τελικός χρήστης έχει επιλέξει να απορρίπτει κλήσεις όταν δεν εμφανίζεται η ταυτότητα του καλούντος, ο πάροχος έχει το δικαίωμα να προσπερνά την επιλογή του αυτή, εφόσον η κλήση προέρχεται από κάποιον οργανισμό έκτακτης ανάγκης.

Το ίδιο συμβαίνει και αναφορικά με την επιλογή του τελικού χρήστη να παρεμποδίζει την επεξεργασία των δεδομένων που βρίσκονται στον τερματικό του εξοπλισμό και αφορούν τα Παγκόσμια Δορυφορικά Συστήματα Πλοήγησης (GNSS), εφόσον πραγματοποιείται μια κλήση προς οργανισμούς έκτακτης ανάγκης.

Με το άρθρο 14 προβλέπεται η δυνατότητα των παρόχων να περιορίζουν τη λήψη από την πλευρά των τελικών χρηστών ανεπιθύμητων, κακόβουλων και ενοχλητικών κλήσεων. Δίδεται δε το δικαίωμα στα κράτη- μέλη να θεσπίσουν πιο συγκεκριμένες διατάξεις για τη διαφάνεια των διαδικασιών σε περίπτωση που ο τελικός χρήστης αιτείται την ανίχνευση μιας ανεπιθύμητης, κακόβουλης ή ενοχλητικής κλήσης.

Στο άρθρο 15 ορίζονται όσα αφορούν στους καταλόγους που είναι διαθέσιμοι στο κοινό. Ήτοι, ορίζεται ότι για την ένταξη των προσωπικών δεδομένων του χρήστη σε καταλόγους που είναι διαθέσιμοι στο κοινό απαιτείται αρχικά η συγκατάθεσή του, αλλά σε περίπτωση που παρόλα αυτά τα κράτη- μέλη θεσπίσουν ειδικότερο νόμο για την συμπερίληψη τέτοιων δεδομένων σε καταλόγους, το φυσικό πρόσωπο το οποίο αυτά αφορούν, δύναται να φέρει αντίρρηση στην συμπερίληψη αυτή. Σε κάθε δε περίπτωση ο τελικός χρήστης διατηρεί τα δικαιώματα που του παρέχει ο ΓΚΠΔ (διόρθωσης, διαγραφής, εναντίωσης) σε σχέση με τα δεδομένα αυτά.

Τέλος, το άρθρο 16 θεσπίζει τους κανόνες αναφορικά με τις επικοινωνίες που λαμβάνουν χώρα για διαφημιστικούς σκοπούς. Ως νόμιμη βάση για να πραγματοποιούνται τέτοιου είδους κλήσεις δίδεται από την παράγραφο 1 του ίδιου άρθρου και δεν είναι άλλη από την προηγούμενη συγκατάθεση του χρήστη. Εάν, όμως, έχει προηγηθεί η πώληση προϊόντων και το φυσικό ή νομικό πρόσωπο αντλεί τα στοιχεία του χρήστη με τον τρόπο αυτό, δύναται να τα χρησιμοποιεί για την άμεση εμπορική προώθηση προϊόντων ή υπηρεσιών, με τη ρητή όμως προϋπόθεση ότι θα δίδεται η δυνατότητα στον χρήστη σαφώς και ευδιάκριτα να αντιτίθεται στην επικοινωνία αυτή. Στα κράτη- μέλη δίνεται η δυνατότητα να ορίσουν ένα συγκεκριμένο χρονικό όριο που ο επικοινωνούν για διαφημιστικούς λόγους μπορεί να διατηρήσει και να αντλήσει τα στοιχεία του χρήστη, μετά την πώληση. Ορίζονται, μάλιστα, ρητά και περιοριστικά από το ίδιο άρθρο οι προϋποθέσεις που θα πρέπει να συντρέχουν ώστε μια τέτοια επικοινωνία να είναι σύννομη, οι οποίες είναι να αποκαλύπτει το φυσικό ή νομικό πρόσωπο το οποίο προβαίνει στην επικοινωνία αυτή την ταυτότητά του, να ενημερώνει τον τελικό χρήστη για τα στοιχεία επικοινωνίας του φυσικού ή νομικού προσώπου από την πλευρά του οποίου γίνεται η επικοινωνία και τέλος σαφώς και ευδιάκριτα πρέπει να δίνεται το δικαίωμα στον τελικό χρήστη

να αντιτίθεται ή να ανακαλεί τη συγκατάθεσή του αναφορικά με τη λήψη τέτοιου είδους επικοινωνιών.

V.4.2. Οι αλλαγές που επήλθαν στο τρίτο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Το κεφάλαιο αυτό αποτελείται από 5 άρθρα, τα οποία, όπως γίνεται εμφανές από τον κατωτέρω συγκριτικό πίνακα των δύο σχεδίων του Κανονισμού, έχει υποστεί επίσης πολλές αλλαγές.

Οι αλλαγές εμφαίνονται εκτενώς κατωτέρω:

CHAPTER III *NATURAL AND LEGAL PERSONS' RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS*	CHAPTER III ***END-USERS'** RIGHTS TO CONTROL ELECTRONIC COMMUNICATIONS*
Article 12 *Presentation and restriction of calling and connected line identification* 1. Where presentation of the calling and connected line identification is offered in accordance with Article [107] of the [Directive establishing the European Electronic Communication Code], the providers of publicly available number-based interpersonal communications services shall provide the following: (a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis; (b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls; (c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user; (d) the called end-user with the possibility of preventing the presentation of the connected line identification to the calling end-user. 2. The possibilities referred to in points (a), (b), (c) and (d) of paragraph 1 shall be provided to end-users by simple means and free of charge. 3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1 shall also apply to incoming calls originating in third countries. 4. Where presentation of calling or connected line identification is offered, providers of publicly available number-based interpersonal communications services shall provide information to the public regarding the options set out in points (a), (b), (c) and (d) of paragraph 1.	Article 12 *Presentation and restriction of calling and connected line identification* 1. Where presentation of the calling and connected line identification is offered in accordance with Article **[115]** of the **Directive (EU) 2018/1972,** the providers of ~~publicly available~~ number-based interpersonal communications services shall provide the following: (a) the calling end-user with the possibility of preventing the presentation of the calling line identification on a per call, per connection or permanent basis; (b) the called end-user with the possibility of preventing the presentation of the calling line identification of incoming calls; (c) the called end-user with the possibility of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling end-user; (d) the called end-user with the possibility of preventing the presentation of the connected line identification **to which** the calling end-user **is connected.** 2. The possibilities referred to in ~~points (a), (b), (c) and (d) of~~ paragraph 1 shall be provided to end-users by simple means and free of charge. 3. Point (a) of paragraph 1 shall also apply with regard to calls to third countries originating in the Union. Points (b), (c) and (d) of paragraph 1 shall also apply to incoming calls originating in third countries. 4. Where presentation of calling or connected line identification is offered, providers of ~~publicly available~~ number-based interpersonal communications services shall provide information to the public regarding the options set out in ~~points (a), (b), (c) and (d) of~~ paragraph 1 **and the exceptions set forth in Article 13.**
Article 13 *Exceptions to presentation and restriction of calling and connected line identification* 1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, where a call is made to emergency services, providers of publicly available number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of metadata, on a per-line basis for	Article 13 *Exceptions to presentation and restriction of calling and connected line identification **in relation to emergency communications*** 1. Regardless of whether the calling end-user has prevented the presentation of the calling line identification, **where emergency communications** are made to emergency services, providers of ~~publicly available~~ number-based interpersonal communications services shall override the elimination of the presentation of the calling line identification and the denial or absence of consent of an end-user for the processing of

organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications. 2. Member States shall establish more specific provisions with regard to the establishment of procedures and the circumstances where providers of publicly available number-based interpersonal communication services shall override the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of malicious or nuisance calls.	metadata, on a per-line basis for organisations dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications. **1a. Regardless whether the called end-user rejects incoming calls where the presentation of the calling line identification has been prevented by the calling end-user, providers of number-based interpersonal communications services shall override this choice, where technically possible, when the calling end-user is an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such communications.** ~~2.~~ **3. Notwithstanding Article 8(1), regardless of whether the end-user has prevented access to the terminal equipment's Global Navigation Satellite Systems (GNSS) capabilities or other types of terminal equipment based location data through the terminal equipment settings, when a call is made to emergency services, such settings may not prevent access to GNSS such location data to determine and provide the caller calling end-user's location to emergency services an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such calls.**
Article 14 *Incoming call blocking* Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted calls by end-users and shall also provide the called end-user with the following possibilities, free of charge: (a) To block incoming calls from specific numbers or from anonymous sources; (b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.	Article 14 *Incoming call blocking* 1. Providers of ~~publicly available~~ number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted, **malicious or nuisance calls by end-users.** **1a. Member States shall establish more specific provisions with regard to the establishment of transparent procedures and the circumstances where providers of number-based interpersonal communication services shall override, or otherwise address, the elimination of the presentation of the calling line identification on a temporary basis, where end-users request the tracing of unwanted, malicious or nuisance calls.** **2. Providers of number-based interpersonal communications services shall also provide the called end-user with the following possibilities, free of charge:** (a) to block, **where technically feasible,** incoming calls from specific numbers or from anonymous sources **or from numbers using a specific code or prefix referred to in Article 16(3a); and** (b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.
Article 15 *Publicly available directories* 1. The providers of publicly available directories shall obtain the consent of end-users who are natural persons to include their personal data in the directory and, consequently, shall obtain consent from these end-users for inclusion of data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. Providers shall give end-users who are natural persons the means to verify, correct and delete such data. 2. The providers of a publicly available directory shall inform end-users who are natural persons whose personal data are in the directory of the available search functions of the directory and obtain end-users' consent before enabling such search functions related to their own data. 3. The providers of publicly available directories shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. Providers	Article 15 *Publicly available directories* 1. The providers of **number-based interpersonal communications services** shall obtain the consent of end-users who are natural persons to include their personal data in the directory and ~~consequently, shall obtain consent from these end-users~~ for inclusion of **such** data per category of personal data, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory. ~~Providers shall give end-users who are natural persons the means to verify, correct and delete such data.~~ **1aa. Notwithstanding paragraph 1, Member States may provide by law that the inclusion of personal data of an end-user who is a natural person in a publicly available directory can take place provided that he end-user who is a natural person shall have the right to object to such inclusion.** 2. The providers of **number-based interpersonal communications services** shall inform end-users who are

shall give such end-users that are legal persons the means to verify, correct and delete such data. 4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge.	natural persons whose personal data are in the directory **of any** search functions **that is not based on name or number in the directory** and obtain ~~end-users'~~ **the** consent **of end-users'** before enabling such search functions related to their own data. 3. The providers of **number-based interpersonal communications services** shall provide end-users that are legal persons with the possibility to object to data related to them being included in the directory. ~~Providers shall give such end-users that are legal persons the means to verify, correct and delete such data.~~ **3a. The providers of number-based interpersonal communications services shall give end-users the means to verify, correct and delete data included in a publicly available directory.** **3aa. Notwithstanding paragraphs 1aa to 3a, Member States may provide by law that the requirements under those paragraphs apply to providers of publicly available directories, in addition to or instead of, providers of number-based interpersonal communications services.** 4. The possibility for end-users not to be included in a publicly available directory, or to verify, correct and delete any data related to them shall be provided free of charge. **4a. Where the personal data of the end-users of number based interpersonal communications services have been included in a publicly available directory before this Regulation enters into force, the personal data of such end-users may remain included in a publicly available directory, including version with search functions, unless the end-users have expressed their objection against their data being included in the directory or against the use of available search functions related to their data.**
Article 16 *Unsolicited communications* 1. Natural or legal persons may use electronic communications services for the purposes of sending direct marketing communications to end-users who are natural persons that have given their consent. 2. Where a natural or legal person obtains electronic contact details for electronic mail from its customer, in the context of the sale of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these electronic contact details for direct marketing of its own similar products or services only if customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection and each time a message is sent. 3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall: (a) present the identity of a line on which they can be contacted; or (b) present a specific code/or prefix identifying the fact that the call is a marketing call. 4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications. 5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to unsolicited communications sent by means set forth under paragraph 1 are sufficiently protected. 6. Any natural or legal person using electronic communications services to transmit direct marketing communications shall	Article 16 *Unsolicited and direct marketing communications* 1. Natural or legal persons **shall be prohibited from using electronic communications services** for the purposes of sending direct marketing communications to end-users who are natural persons **unless** they have given their **prior** consent. 2. **Notwithstanding paragraph 1,** where a natural or legal person obtains contact details for electronic **message from end-users who are natural persons,** in the context of **the purchase** of a product or a service, in accordance with Regulation (EU) 2016/679, that natural or legal person may use these ~~electronic~~ contact details for direct marketing of its own similar products or services only if such **end-users** are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use. The right to object shall be given at the time of collection **of such end-users' contact details and, if that end-user has not initially refused that use, each time when a natural or legal persons sends a message to that end-user for the purpose of such direct marketing.** **2a. Member States may provide by law a set period of time, after the sale of the product or service occurred, within which a natural or legal person may use contact details of the end-user who is a natural person for direct marketing purposes, as provided for in paragraph.** 3. Without prejudice to paragraphs 1 and 2, natural or legal persons using electronic communications services for the purposes of placing direct marketing calls shall present **the calling line identification assigned to them.** **3a. Member States may require natural or legal person using electronic communications services for the purposes of placing direct marketing calls to present a specific code or prefix identifying the fact that the call is a direct marketing call in addition to the obligation set out in paragraph 3. Member State requiring the use of such a specific code or prefix shall make it available for the natural or legal persons**

inform end-users of the marketing nature of the communication and the identity of the legal or natural person on behalf of whom the communication is transmitted and shall provide the necessary information for recipients to exercise their right to withdraw their consent, in an easy manner, to receiving further marketing communications. 7. The Commission shall be empowered to adopt implementing measures in accordance with Article 26(2) specifying the code/or prefix to identify marketing calls, pursuant to point (b) of paragraph 3.	**who use electronic communications services for the purposes of direct marketing calls.** 4. Notwithstanding paragraph 1, Member States may provide by law that the placing of direct marketing voice-to-voice calls to end-users who are natural persons shall only be allowed in respect of end-users who are natural persons who have not expressed their objection to receiving those communications. 5. Member States shall ensure, in the framework of Union law and applicable national law, that the legitimate interest of end-users that are legal persons with regard to **direct marketing** communications sent by means set forth under paragraph 1 are sufficiently protected. 6. Any natural or legal person using electronic communications services to **send** direct marketing communications shall, **each time a direct marketing communication is sent:** **(a) reveal his or its identity and use effective return addresses or numbers;** **(b) inform end-users of the marketing nature of the communication and the identity and contact details of the legal or natural person on behalf of whom the direct marketing communication is sent;** ~~(c)~~ **(d) clearly and distinctly give the end-users who are natural persons a means to object or to withdraw their consent, free of charge, at any time, and in an easy and effective manner, to receiving further direct marketing communications, and shall provide the necessary information to this end. This means shall also be given at the time of collection of the contact details according to paragraph 2. It shall be as easy to withdraw as to give consent.** ~~7.~~
Article 17 *Information about detected security risks* In the case of a particular risk that may compromise the security of networks and electronic communications services, the provider of an electronic communications service shall inform end-users concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, inform end-users of any possible remedies, including an indication of the likely costs involved.	~~Article 17~~ ~~*Information about detected security risks*~~

Πίνακας 3: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Στο παρόν κεφάλαιο, εντοπίζεται αρχικά από τον ανωτέρω συγκριτικό πίνακα, η μείωση των άρθρων, ο αριθμός των οποίων στο πρώτο σχέδιο του Κανονισμού ήταν 6 και στο δεύτερο έγιναν πέντε 5, αφού διεγράφη το άρθρο με τον αριθμό 17.

Εντοπίζεται και πάλι διαφορά στον τίτλο του κεφαλαίου, όπου τα φυσικά και νομικά πρόσωπα αντικαταστάθηκαν από τον όρο «τελικοί χρήστες». Με τις τροποποιήσεις που πραγματοποιήθηκαν έως και σήμερα στο παρόν κεφάλαιο φαίνεται να έχουν γίνει βήματα προς την περαιτέρω προστασία των τελικών χρηστών μέσω της αύξησης των δικαιωμάτων τους με την παράλληλη αύξηση των υποχρεώσεων των παρόχων.

Σημαντικότερες αλλαγές εντοπίζονται κατ' αρχάς στο άρθρο 13, στο οποίο προστέθηκαν δύο παράγραφοι, η 1α και η 3, ενώ διεγράφη η παράγραφος 2. Με την παράγραφο 1α έγινε προσθήκη του δικαιώματος των παρόχων να προσπερνούν την επιλογή του χρήστη να απορρίπτει τις κλήσεις όταν δεν εμφαίνεται η ταυτότητα του καλούντος, σε περίπτωση που καλεί οργανισμός έκτακτης ανάγκης και με την παράγραφο 3 έγινε προσθήκη του δικαιώματος του παρόχου, εφόσον ο τελικός χρήστης έχει επιλέξει να παρεμποδίζει την επεξεργασία των δεδομένων που βρίσκονται στον τερματικό του εξοπλισμό και αφορούν τα Παγκόσμια Δορυφορικά Συστήματα Πλοήγησης (GNSS), να παρακάμπτει την επιλογή του αυτή εάν ο τελικός χρήστης πραγματοποιήσει μια κλήση έκτακτης ανάγκης.

Μια παράγραφος προστέθηκε και στο άρθρο 14 (βλ. Άρθρο 14 § 1^{α}- 2^{ου} σχεδίου), η οποία παρέχει τη διακριτική ευχέρεια στα κράτη- μέλη να θεσπίζουν πιο συγκεκριμένες διατάξεις αναφορικά με τη δυνατότητα των παρόχων να παρακάμπτουν τη μη παρουσίαση της ταυτότητας της καλούσας γραμμής όταν ο τελικός χρήστης αιτηθεί τον εντοπισμό ανεπιθύμητων, κακόβουλων ή ενοχλητικών κλήσεων.

Ενδιαφέρον παρουσιάζει η αλλαγή στο άρθρο 15, το οποίο προέβλεπε ως μόνη νομική βάση για την ένταξη των προσωπικών δεδομένων ενός τελικού χρήστη σε διαθέσιμους στο κοινό καταλόγους τη συγκατάθεσή του ενώ στο τελευταίο σχέδιο του Κανονισμού βλέπουμε ότι προστέθηκε με την παράγραφο 1αα η δυνατότητα στα κράτη- μέλη να προβλέπουν δια νόμου την συμπερίληψη προσωπικών δεδομένων των τελικών χρηστών σε καταλόγους διαθέσιμους στο κοινό, δίνοντας στον τελικό χρήστη το δικαίωμα της εναντίωσης στη συνέχεια.

Προς την αντίθετη κατεύθυνση κινήθηκε η προστιθέμενη στο άρθρο 16 παράγραφος 2α, η οποία προβλέπει ότι κατά τη διακριτική ευχέρεια των κρατών- μελών μπορούν τα τελευταία να προβλέψουν συγκεκριμένη περίοδο μετά την αγορά προϊόντων ή υπηρεσιών κατά την οποία θα μπορούν οι πωλητές να χρησιμοποιούν τα δεδομένα των υποκειμένων για διαφημιστικούς σκοπούς. Επίσης, προστέθηκε η πρόβλεψη με την παράγραφο 3α τα κράτη- μέλη να ζητούν από τους καλούντες για διαφημιστικούς σκοπούς να χρησιμοποιούν έναν συγκεκριμένο κωδικό με σκοπό να γνωρίζουν οι τελικοί χρήστες ότι πρόκειται για τέτοιου είδους κλήσεις. Προστέθηκαν, τέλος, στο ίδιο άρθρο οι υποχρεώσεις των καλούντων για διαφημιστικούς λόγους, ώστε να θεωρηθεί μια τέτοια επικοινωνία σύννομη.

V.5. Κεφάλαιο τέταρτο- Ανεξάρτητες Εποπτικές Αρχές και Επιβολή

V.5.1. Οι ειδικότερες ρυθμίσεις του τέταρτου κεφαλαίου

Στο κεφάλαιο τέταρτο του Κανονισμού εντοπίζουμε τις ρυθμίσεις που αφορούν την Ανεξάρτητη Εποπτική Αρχή ή τις Ανεξάρτητες Εποπτικές Αρχές, που θα παρακολουθεί ή θα παρακολουθούν την εφαρμογή του Κανονισμού (άρθρο 18), το Ευρωπαϊκό Συμβούλιο Προσωπικών Δεδομένων και τον ρόλο του (άρθρο 19) και τη διασυνοριακή συνεργασία των Αρχών (άρθρο 20).

Με το άρθρο 18 του Κανονισμού εισάγεται η υποχρέωση των κρατών- μελών να ορίσουν Ανεξάρτητη Εποπτική Αρχή για την καλύτερη δυνατή εφαρμογή του Κανονισμού, η οποία δύναται να είναι η ίδια με αυτή που είναι υπεύθυνη για την εφαρμογή του ΓΚΠΔ ή διαφορετική. Σε περίπτωση που δεν είναι η ίδια Αρχή υπεύθυνη για την εφαρμογή του παρόντος Κανονισμού και του ΓΚΠΔ, θα πρέπει οι Αρχές να συνεργάζονται μεταξύ τους. Η επιλεγείσα Αρχή όμως οφείλει να έχει το δικαίωμα να επιβάλει πρόστιμα στους παραβάτες. Στη χώρα μας, ενώ το εύλογο θα ήταν να επωμιστεί την υποχρέωση εποπτείας της τήρησης του Κανονισμού πιθανότατα η ΑΔΑΕ, ως ειδικότερη στα ζητήματα των επικοινωνιών, μάλλον η ΑΠΔΠΧ, ως υπεύθυνη για τα ζητήματα που ανακύπτουν στο πεδίο του ΓΚΠΔ, θα είναι τελικά αυτή που θα αναλάβει και το έργο αυτό αναφορικά με τον Κανονισμό ePrivacy, έτσι ώστε να υπάρχει και μια λογική αλληλουχία στα ανακύπτοντα αυτά ζητήματα.

Με το άρθρο 19, το οποίο αφορά στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και στα καθήκοντα που αυτό θα έχει σε σχέση με την εφαρμογή του Κανονισμού, τα οποία θα είναι να συμβουλεύει την Επιτροπή σχετικά με την τροποποίησή του, να εξετάζει κάθε ζήτημα που αφορά στην εφαρμογή του, να εκδίδει κατευθύνσεις, συστάσεις κ.λπ. και να εκδίδει κατευθυντήριες γραμμές, συστάσεις κ.λπ. σε σχέση με τη συνεργασία των ανεξάρτητων Αρχών, εφόσον αυτές είναι διαφορετικές για την εφαρμογή του παρόντος και την εφαρμογή του ΓΚΠΔ κ.ά. Ο ρόλος του Συμβουλίου, όπως αποτυπώνεται στο άρθρο αυτό, γίνεται αντιληπτό ότι είναι αμιγώς συμβουλευτικός και στοχεύει στη διευκόλυνση προς την καλύτερη εφαρμογή του Κανονισμού.

Στο άρθρο 20 ρυθμίζεται η διασυνοριακή συνεργασία, ορίζοντας ότι κάθε Αρχή θα πρέπει να συμβάλλει στη συνεκτική εφαρμογή του υπό μελέτη Κανονισμού σε ολόκληρη την Ένωση και να υπάρχει παράλληλη συνεργασία και με την Ευρωπαϊκή Επιτροπή.

V.5.2. Οι αλλαγές που επήλθαν στο τέταρτο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Στο κεφάλαιο αυτό του Κανονισμού εντοπίζουμε τις ρυθμίσεις που σχετίζονται με την ανεξάρτητη Αρχή που θα επωμιστεί την ευθύνη για την ορθή εφαρμογή του Κανονισμού καθώς και τις αρμοδιότητες και τον ρόλο που θα διαδραματίζει το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων στην εφαρμογή του Κανονισμού. Εάν και το εν λόγω κεφάλαιο είναι σχετικά μικρό, παρατηρούνται αρκετές αλλαγές στο περιεχόμενό του.

Ειδικότερα, οι αλλαγές στο κεφάλαιο αυτό έχουν ως κατωτέρω:

CHAPTER IV *INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT*	*CHAPTER IV* *INDEPENDENT SUPERVISORY AUTHORITIES AND ENFORCEMENT*
Article 18 *Independent supervisory authorities* 1. The independent supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring the application of this Regulation. Chapter VI and VII of Regulation (EU) 2016/679 shall apply mutatis mutandis. The tasks and powers of the supervisory authorities shall be exercised with regard to end-users. 2. The supervisory authority or authorities referred to in paragraph 1 shall cooperate whenever appropriate with national regulatory authorities established pursuant to the [Directive Establishing the European Electronic Communications Code].	Article 18 *Ssupervisory authorities* **0. Each Member State shall provide for one or more independent public authorities meeting the requirements set out in Articles 51 to 54 of Regulation (EU) 2016/679 to be responsible for monitoring the application of this Regulation.** **Member States may entrust the monitoring of the application of Articles 12 to 16 to the supervisory authority or authorities referred to in the previous subparagraph or to another supervisory authority or authorities having the appropriate expertise.** ~~1.~~ 1ab. The supervisory ~~authority or~~ authorities **shall have investigative and corrective powers, including the power to impose administrative fines pursuant to article 23.** **1b. Where more than one supervisory authority is responsible for monitoring the application of this Regulation in a Member State, such authorities shall cooperate with each other to the extent necessary to perform their tasks.** **2. Where the supervisory authorities are not the supervisory authorities responsible for monitoring the application of Regulation (EU) 2016/679, theynshall cooperate with the latter and, whenever appropriate, with national regulatory authorities established pursuant to Directive (EU) 2018/1972 and other relevant authorities.**
Article 19 *European Data Protection Board* The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, shall have competence to ensure the consistent application of this Regulation. To that end, the European Data Protection Board shall exercise the tasks laid down in Article 70 of Regulation (EU) 2016/679. The Board shall also have the following tasks: (a) advise the Commission on any proposed amendment of this Regulation; (b) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation.	Article 19 *European Data Protection Board* 1. The European Data Protection Board, established under Article 68 of Regulation (EU) 2016/679, **shall have the task to contribute to the consistent application of Chapters I and II and III of this Regulation.** 2. **To that end**, the Board shall have the following tasks: (a) advise the Commission on any proposed amendment of this Regulation; (b) examine, on its own initiative, **on request of a supervisory authority designated in accordance with Article 18 (0) or** on request of the Commission, any question covering the application of this Regulation **in relation to Chapters I, II and III** and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation; ~~(c)~~ **(d) issue guidelines, recommendations and best practices in order to facilitate cooperation, including exchange of information, between supervisory authorities referred to in paragraph 0 of Article 18 and/or the supervisory authority**

	responsible for monitoring the application of Regulation (EU) 2016/679; **(da) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph to assess for different types of electronic communications services the moment in time of receipt of electronic communications content;** **(db) issue guidelines, recommendations and best practices in accordance with point (b) of this paragraph on the provision of consent in the context of Articles 6 to 6b and 8 of this Regulation by end-users who are legal persons and or in an employment relationship;** **(e) provide the Commission with an opinion on the icons referred to in paragraph 3 of Article 8;** ~~**(f)**~~ ~~**(g)**~~ **(h) promote the exchange of knowledge and documentation on legislation on protection of electronic communications of end-users and of the integrity of their terminal equipment as laid down in Chapter II and practice relevant supervisory authorities world wide;** **3. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.** **4. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.** **5. The Board shall consult the supervisory authorities referred to in Article 18 (0) before any of the tasks referred to in paragraph 2.** **6. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76 of Regulation (EU) 2016/679, make the result of the consultation procedures publicly available.**
Article 20 *Cooperation and consistency procedures* Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For this purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.	Article 20 *Cross-border cooperation* Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union **and** cooperate with each other and with the Commission ~~**in accordance with Chapter VII of Regulation (EU) 2016/679 regarding the matters covered by this Regulation.**~~

Πίνακας 4: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Στο άρθρο 18 του πρώτου σχεδίου του Κανονισμού προβλέφθηκε ότι η Αρχή η οποία είναι υπεύθυνη και για την ορθή εφαρμογή του ΓΚΠΔ θα είναι υπεύθυνη και για την ορθή εφαρμογή του υπό εξέταση Κανονισμού, ενώ αντίθετα στο πιο πρόσφατο σχέδιο δόθηκε η δυνατότητα στα κράτη- μέλη να επιφορτίσουν, εφόσον το επιθυμούν, έτερη ανεξάρτητη Αρχή με την ευθύνη της ορθής εφαρμογής του υπό εξέταση Κανονισμού (βλ. Άρθρο 18 § 0).

Επίσης, στο άρθρο 19, στο δεύτερο σχέδιο του Κανονισμού, εντοπίζεται σημαντική αύξηση των αρμοδιοτήτων του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σε σχέση με τα καθήκοντα που του είχαν αρχικώς δοθεί, οι οποίες από δύο (2) πλέον ανέρχονται στις επτά (7) (βλ. Άρθρο 19 § 2).

Τέλος, στο άρθρο 20 εντοπίζεται η διαγραφή της πρόβλεψης ότι η συνεργασία των ανεξάρτητων Αρχών θα πρέπει να γίνεται σύμφωνα με το κεφάλαιο 7 του ΓΚΠΔ (Συνεργασία εποπτικών Αρχών, συνεκτικότητα κ.λπ.) και πλέον ορίζεται ότι η εκάστοτε Αρχή οφείλει να συνεργάζεται και με την Ευρωπαϊκή Επιτροπή (βλ. Άρθρο 20).

V.6. Κεφάλαιο πέμπτο- Προσφυγές, Ευθύνη και Κυρώσεις

V.6.1. Οι ειδικότερες ρυθμίσεις του πέμπτου κεφαλαίου

Στο πέμπτο κεφάλαιο εντοπίζονται ρυθμίσεις αναφορικά με τις προσφυγές στις οποίες μπορεί να προχωρήσει ο τελικός χρήστης σε περίπτωση που θιγούν τα δικαιώματά του που απορρέουν από τον Κανονισμό (άρθρο 21), με το δικαίωμα αποζημίωσης το οποίο διατηρεί ο τελικός χρήστης και της ευθύνης (άρθρο 22), με τους γενικούς όρους επιβολής διοικητικών προστίμων (άρθρο 23) και τέλος με τις κυρώσεις (άρθρο 24).

Δίνεται το δικαίωμα στους θιγόμενους τελικούς χρήστες να προχωρήσουν σε καταγγελία ενώπιον της αρμόδιας εποπτικής Αρχής, εφόσον θιγούν τα δικαιώματά τους, με το άρθρο 21, καθώς και δικαίωμα να στραφεί με δικαστικά μέσα κατά οποιασδήποτε δεσμευτικής απόφασης που θα εκδοθεί από την Αρχή. Παράλληλα, προβλέπεται η εφαρμογή των άρθρων 77- 80 του ΓΚΠΔ και, τέλος, το δικαίωμα κάθε φυσικού ή νομικού προσώπου, συμπεριλαμβανομένων των παρόχων ηλεκτρονικών επικοινωνιών να χαίρουν προστασίας ενάντια σε οποιαδήποτε παραβίαση.

Δυνάμει του άρθρου 22 θεσπίζεται το δικαίωμα αποζημίωσης για τα άτομα τα οποία υπέστησαν οποιαδήποτε υλική ή μη υλική ζημία ως αποτέλεσμα παραβίασης του υπό μελέτη Κανονισμού από τον υπαίτιο της ζημίας αυτής, σύμφωνα με τα όσα ορίζονται στο άρθρο 82 του ΓΚΠΔ.

Με το άρθρο 23 ορίζονται οι γενικοί όροι που ισχύουν για την επιβολή των εκάστοτε διοικητικών προστίμων. Αρχικά, το εν λόγω άρθρο παραπέμπει σχετικά στο άρθρο 83 του ΓΚΠΔ[148] και εν συνεχεία προβλέπει το ύψος των προστίμων σε περίπτωση παραβάσεων των

[148] Βλ. Άρθρο 83 ΓΚΠΔ (ΕΕ) 2016/679 «*Γενικοί όροι επιβολής διοικητικών προστίμων*».

υποχρεώσεων κάθε προσώπου φυσικού ή νομικού το οποίο επεξεργάζεται δεδομένα ηλεκτρονικών επικοινωνιών, των υποχρεώσεων των παρόχων λογισμικού το οποίο παρέχει τη δυνατότητα πραγματοποίησης ηλεκτρονικών επικοινωνιών, των υποχρεώσεων των παρόχων διαθέσιμων στο κοινό καταλόγων, των υποχρεώσεων κάθε προσώπου φυσικού ή νομικού το οποίο κάνει χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών, σε περίπτωση παραβίασης του απορρήτου των επικοινωνιών και σε περίπτωση μη συμμόρφωσης με εντολή/ απόφαση της αρμόδιας εποπτικής Αρχής.

Με το άρθρο 24 ορίζεται ότι τα κράτη- μέλη κατά τη διακριτική τους ευχέρεια θεσπίζουν τους κανόνες εκείνους που σχετίζονται με τις παραβάσεις που δεν δύνανται να αποτελέσουν αντικείμενο διοικητικών προστίμων, σύμφωνα με τα όσα ορίστηκαν ανωτέρω και λαμβάνουν βέβαια τα απαραίτητα και κατάλληλα μέτρα προς την εφαρμογή των κανόνων αυτών. Οι κανόνες αυτοί πάντως θα πρέπει να κοινοποιηθούν στην Επιτροπή, σε ρητά ορισμένο χρονικό πλαίσιο, σύμφωνα με την παράγραφο 2 του ίδιου άρθρου.

V.6.2. Οι αλλαγές που επήλθαν στο πέμπτο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Στο παρόν κεφάλαιο δεν έχουν επέλθει δραματικές αλλαγές σε σχέση με το τελευταίο σχέδιο του Κανονισμού, ως εμφαίνεται εκτενώς κατωτέρω.

Ειδικότερα:

CHAPTER V *REMEDIES, LIABILITY AND PENALTIES*	*CHAPTER V* *REMEDIES, LIABILITY AND PENALTIES*
Article 21 *Remedies* 1. Without prejudice to any other administrative or judicial remedy, every end-user of electronic communications services shall have the same remedies provided for in Articles 77, 78, and 79 of Regulation (EU) 2016/679. 2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation and having a legitimate interest in the cessation or prohibition of alleged infringements, including a provider of electronic communications services protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.	Article 21 *Remedies* 1. Without prejudice to any other administrative or judicial remedy, every end-user **shall have the right to an effective judicial remedy in relation to any infringement of rights under this Regulation, the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy against any legally binding decision of a supervisory authority concerning them.** 1a. Articles 77-80 of Regulation (EU) 2016/679 **shall apply mutatis mutandis.** 2. Any natural or legal person other than end-users adversely affected by infringements of this Regulation, **including a provider of electronic communications services** protecting its legitimate business interests, shall have a right to bring legal proceedings in respect of such infringements.
Article 22 *Right to compensation and liability* Any end-user of electronic communications services who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered, unless the infringer proves that it is not in any way responsible for the	Article 22 *Right to compensation and liability* Any ~~end-user of electronic communications~~ **person** who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the infringer for the damage suffered ~~unless the infringer proves that it is not in any way responsible for the~~

event giving rise to the damage in accordance with Article 82 of Regulation (EU) 2016/679.	~~event giving rise to the damage~~ in accordance with Article 82 of Regulation (EU) 2016/679.
Article 23 *General conditions for imposing administrative fines* 1. For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679 shall apply to infringements of this Regulation. 2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8; (b) the obligations of the provider of software enabling electronic communications, pursuant to Article 10; (c) the obligations of the providers of publicly available directories pursuant to Article 15; (d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16. 3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. 4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13, 14, and 17. 5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. 6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. 7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process. 8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.	Article 23 *General conditions for imposing administrative fines* 1. ~~For the purpose of this Article, Chapter VII of Regulation (EU) 2016/679~~ **Article 83 of Regulation (EU) 2016/679** shall apply **mutatis mutandis** to infringements of this Regulation. 2. Infringements of the following provisions of this Regulation shall, in accordance with paragraph 1, be subject to administrative fines up to EUR 10 000 000, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of any legal or natural person who process electronic communications data pursuant to Article 8; ~~(b)~~ (c) the obligations of the providers of publicly available directories pursuant to Article 15; (d) the obligations of any legal or natural person who uses electronic communications services pursuant to Article 16. (e) the obligation to designate a representative pursuant to Article 3 number 2. 3. Infringements of the principle of confidentiality of communications, permitted processing of electronic communications data, time limits for erasure pursuant to Articles 5, 6, and 7 shall, in accordance with paragraph 1 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. 4. Member States shall lay down the rules on penalties for infringements of Articles 12, 13 and 14 ~~and 17~~. 5. Non-compliance with an order by a supervisory authority as referred to in Article 18, shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. 6. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 18, each Member State may lay down rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. 7. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process. 8. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by [xxx] and, without delay, any subsequent amendment law or amendment affecting them.
Article 24 *Penalties* 1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to	Article 24 *Penalties* 1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 23, and shall take all measures necessary to

ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive. 2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than 18 months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.	ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive. 2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, no later than **8** months after the date set forth under Article 29(2) and, without delay, any subsequent amendment affecting them.

Πίνακας 5: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Αξιοσημείωτες είναι οι αλλαγές αναφορικά με τις παραπομπές στον ΓΚΠΔ 2016/679. Σύμφωνα με το νέο σχέδιο η εφαρμογή του ΓΚΠΔ στο πλαίσιο των προσφυγών και της επιβολής διοικητικών προστίμων, πρέπει να γίνεται «mutatis mutandis», επιφύλαξη η οποία δεν υπήρχε στο πρώτο σχέδιο του Κανονισμού (βλ. Άρθρο 21 § 1α).

Επίσης, μείζονος σημασίας αλλαγή είναι ότι ως δικαιούχος αποζημίωσης, σύμφωνα με το άρθρο 22, ορίζεται πλέον οποιοδήποτε πρόσωπο υπέστη υλική ή ηθική ζημία, ακόμη και ο πάροχος ηλεκτρονικών επικοινωνιών και όχι μόνο ο τελικός χρήστης των ηλεκτρονικών επικοινωνιών, όπως είχε αρχικώς οριστεί.

V.7. Κεφάλαιο έκτο- Κατ' εξουσιοδότηση Πράξεις και Εκτελεστικές Πράξεις

V.7.1. Οι ειδικότερες ρυθμίσεις του έκτου κεφαλαίου

Το προτελευταίο κεφάλαιο του Κανονισμού αποτελείται από συνολικά 2 άρθρα, τα οποία ορίζουν το μεν πρώτο τη ανάθεση της εξουσίας στην Επιτροπή να εκδίδει κατ' εξουσιοδότηση πράξεις, υπό τους όρους που προβλέπονται στο ίδιο άρθρο (άρθρο 25) και το δεύτερο ορίζει ότι η Επιτροπή επικουρείται από την Επιτροπή Επικοινωνιών και ότι όταν θα γίνεται παραπομπή στο άρθρο αυτό, θα εφαρμόζεται το άρθρο 5 του Κανονισμού (ΕΕ) 182/2011[149] (άρθρο 26).

Έτσι το άρθρο 25 ορίζει ότι η Επιτροπή έχει την εξουσία να εκδίδει κατ' εξουσιοδότηση πράξεις για αόριστο χρονικό διάστημα, έως να ανακληθεί η εξουσία αυτή από το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο, εφόσον προηγουμένως η ίδια διαβουλεύεται με εμπειρογνώμονες, ορισμένοι από κάθε κράτος- μέλος, εφόσον μετά την έκδοση της πράξης την κοινοποιήσει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Οι πράξεις αυτές τίθενται σε ισχύ εφόσον το Ευρωπαϊκό Κοινοβούλιο ή το Συμβούλιο δεν προβάλει αντιρρήσεις.

[149] Ο Κανονισμός (ΕΕ) 182/2011 διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32011R0182&from=BG

Στο άρθρο 26 ορίζονται τα σχετικά με την Επιτροπή, ήτοι ότι αυτή επικουρείται από την επιτροπή επικοινωνιών, η οποία συστάθηκε σύμφωνα με το άρθρο 110 της Οδηγίας 2018/1972 καθώς και ότι όταν γίνεται παραπομπή στην παράγραφο αυτή, θα τυγχάνει εφαρμογής το άρθρο 5 του Κανονισμού (ΕΕ) 182/2011.

V.7.2. Οι αλλαγές που επήλθαν στο έκτο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Στο παρόν κεφάλαιο, λίγο πριν το τέλος του Κανονισμού, δεν εντοπίζεται σχεδόν καμία αλλαγή μεταξύ των δύο σχεδίων.

Πιο συγκεκριμένα:

CHAPTER VI *DELEGATED ACTS AND IMPLEMENTING ACTS*	*CHAPTER VI* *DELEGATED ACTS AND IMPLEMENTING ACTS*
Article 25 *Exercise of the delegation*	Article 25 *Exercise of the delegation*
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].	2. The power to adopt delegated acts referred to in Article 8(4) shall be conferred on the Commission for an indeterminate period of time from [the data of entering into force of this Regulation].
3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. The delegation of power referred to in Article 8(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement on Better Law-Making of 13 April 2016.	4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.
5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.	6. A delegated act adopted pursuant to Article 8(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.
Article 26 *Committee*	Article 26 *Committee*
1. The Commission shall be assisted by the Communications Committee established under Article 110 of the [Directive establishing the European Electronic Communications Code]. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. The Commission shall be assisted by the Communications Committee established under **Article 118 of Directive (EU) 2018/1972.** That committee shall be a committee within the meaning of Regulation (EU) No 182/2011[1].
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Πίνακας 6: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Η μόνη αλλαγή μεταξύ των δύο ως άνω σχεδίων εντοπίζεται στο άρθρο 26 § 1, όπου το πρώτο σχέδιο αναφέρει ότι «*Η Επιτροπή θα πρέπει να επικουρείται από την επιτροπή επικοινωνιών που έχει συσταθεί σύμφωνα με το άρθρο 110 της [οδηγίας για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών] […]*», ενώ το τελευταίο σχέδιο του Κανονισμού αναφέρει ότι «*Η Επιτροπή θα πρέπει να επικουρείται από την Επιτροπή Επικοινωνιών που έχει συσταθεί σύμφωνα με το άρθρο 118 της Οδηγίας (ΕΕ) 2018/1972. […]*».

V.8. Κεφάλαιο έβδομο- Τελικές Διατάξεις

V.8.1. Οι ειδικότερες ρυθμίσεις του έβδομου κεφαλαίου

Στο τελευταίο κεφάλαιο εντοπίζουμε την κατάργηση της οδηγίας 2002/58/ΕΚ (άρθρο 27), την υποχρέωση της Επιτροπής να καταρτίσει λεπτομερές πρόγραμμα για τον έλεγχο της αποτελεσματικότητας του Κανονισμού καθώς και να προβαίνει σε αξιολόγησή του ανά τριετία, υποβάλλοντας τα κύρια πορίσματα ενώπιον του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής (άρθρο 28) και την έναρξη ισχύος του Κανονισμού και εφαρμογή του Κανονισμού (άρθρο 29).

Με το άρθρο 27 καταργείται η οδηγία 2002/58/ΕΚ, θέτοντας μάλιστα ως ενδεικτική ημερομηνία κατάργησης την 1η Αυγούστου 2022. Ακόμη, αναφέρει ότι από την κατάργησή της, οποιαδήποτε παραπομπή γίνεται σε αυτή, νοείται ως παραπομπή στον Κανονισμό.

Το άρθρο 28 ορίζει ότι η Επιτροπή είναι υποχρεωμένη να συντάξει λεπτομερές πρόγραμμα για τον έλεγχο της αποτελεσματικότητας του Κανονισμού, θέτοντας ως ενδεικτική ημερομηνία την 1η Αυγούστου 2024. Εισάγεται, τέλος, η υποχρέωση της Επιτροπής να προβαίνει σε αξιολόγηση του Κανονισμού και να υποβάλλει τα πορίσματά της στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο και στην Ευρωπαϊκή Οικονομική Επιτροπή, για πρώτη φορά το αργότερο τρία έτη από την ημερομηνία εφαρμογής του Κανονισμού και εν συνεχεία ανά τρία έτη. Παράλληλα δύναται να προτείνει τυχόν τροποποιήσεις ή/ και την κατάργηση του Κανονισμού σε συνέχεια νομικών, τεχνικών και οικονομικών εξελίξεων.

Με το τελευταίο άρθρο του Κανονισμού, το άρθρο 29 ορίζεται η έναρξη ισχύος του Κανονισμού, η οποία είναι η εικοστή ημέρα από τη δημοσίευσή του στην Επίσημη Εφημερίδα

της Ευρωπαϊκής Ένωσης. Τέλος, ορίζεται ότι ο Κανονισμός θα αρχίσει να εφαρμόζεται 24 μήνες μετά την έναρξη ισχύος του.

V.8.2. Οι αλλαγές που επήλθαν στο έβδομο κεφάλαιο του Κανονισμού από το πρώτο σχέδιο τον 01.2017 έως το σχέδιο του 02.2021

Εάν και, όπως εμφαίνεται κατωτέρω, στις τελικές διατάξεις του Κανονισμού δεν επήλθαν αλλαγές ως προς τα λοιπά, είναι άξιες αναφοράς οι αλλαγές στις ημερομηνίες εφαρμογής του Κανονισμού.

Αναλυτικότερα:

CHAPTER VII *FINAL PROVISIONS*	*CHAPTER VII* *FINAL PROVISIONS*
Article 27 *Repeal* 1. Directive 2002/58/EC is repealed with effect from 25 May 2018. 2. References to the repealed Directive shall be construed as references to this Regulation.	Article 27 *Repeal* 1. Directive 2002/58/EC is repealed with effect from **[1August 2022].** 2. References to the repealed Directive shall be construed as references to this Regulation.
Article 28 *Monitoring and evaluation clause* By 1 January 2018 at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation. No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.	Article 28 *Monitoring and evaluation clause* By **[1 August 2024]** at the latest, the Commission shall establish a detailed programme for monitoring the effectiveness of this Regulation. No later than three years after the date of application of this Regulation, and every three years thereafter, the Commission shall carry out an evaluation of this Regulation and present the main findings to the European Parliament, the Council and the European Economic and Social Committee. The evaluation shall, where appropriate, inform a proposal for the amendment or repeal of this Regulation in light of legal, technical or economic developments.
Article 29 *Entry into force and application* 1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. It shall apply from 25 May 2018.	Article 29 *Entry into force and application* 1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. This Regulation shall apply from **[24 months from the date of entry into force of this Regulation]**.

Πίνακας 7: Αριστερά εμφαίνεται το από 01.2017 σχέδιο του Κανονισμού και δεξιά το από 02.2021 σχέδιο. Οι προσθήκες ή οι αλλαγές στο σχέδιο του 02.2021 εμφαίνονται με bold, ενώ υπάρχουν και διεγραμμένες διατάξεις ή μεμονωμένες ρυθμίσεις.

Στο αρχικό σχέδιο φαίνεται ότι υπήρξε πρόβλεψη ότι η Οδηγία 2002/58/ΕΚ καταργείται από 25.05.2018 και ο Κανονισμός τίθεται σε ισχύ κατά την ίδια ως άνω ημερομηνία, όταν δηλαδή τέθηκε σε εφαρμογή και ο ΓΚΠΔ[150] (βλ. Άρθρο 27 § 1 - 1ου σχεδίου), ενώ στο τελευταίο σχέδιο ως

[150] Βλ. Άρθρο 99 παρ. 2 ΓΚΠΔ 2016/679: «*Τίθεται σε εφαρμογή από τις 25 Μαΐου 2018*».

ενδεικτική ημερομηνία τίθεται η 1η Αυγούστου 2022 (βλ. Άρθρο 27 § 1- 2ου σχεδίου). Αντίστοιχα, τέθηκε από το πρώτο σχέδιο ως ημερομηνία κατά την οποία η Επιτροπή οφείλει να καταρτίσει λεπτομερές πρόγραμμα για τον έλεγχο της αποτελεσματικότητας του Κανονισμού το αργότερο έως την 1η Ιανουαρίου 2018 (βλ. Άρθρο 28 § 1- 1ου σχεδίου) ενώ από το δεύτερο ενδεικτική ημερομηνία η 1η Αυγούστου 2024 (βλ. Άρθρο 28 § 1 - 2ου σχεδίου). Στην τελική διάταξη του Κανονισμού εντοπίζεται ότι από 25.05.2018, ημερομηνία κατά την οποία θα ετίθετο σε εφαρμογή ο Κανονισμός, σύμφωνα με το πρώτο σχέδιο (βλ. Άρθρο 29 § 2- 1ου σχεδίου), η ημερομηνία τροποποιήθηκε ως εξής: «*24 μήνες από την ημερομηνία της έναρξης ισχύος του Κανονισμού*» (βλ. Άρθρο 29 § 2- 1ου σχεδίου).

VI. Η ΘΕΣΗ ΣΕ ΙΣΧΥ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

VI.1. Οι διαπραγματεύσεις προς την ψήφιση του Κανονισμού

Το πρώτο σχέδιο του Κανονισμού έγινε γνωστό κατά τον πρώτο μήνα του 2017, ωστόσο το 2021 εκδόθηκε το σχέδιο στο οποίο, επιτέλους, συμφώνησαν τα απαρτίζοντα κράτη- μέλη το Συμβούλιο της Ένωσης. Στο μεσοδιάστημα πραγματοποιήθηκε τεράστιος αριθμός διαβουλεύσεων, εκδόθηκαν γνωμοδοτήσεις από την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων, διατυπώθηκαν απόψεις από τα κράτη- μέλη και το κείμενο του Κανονισμού υπέστη πολλές μετατροπές[151].

Συνολικά 8 κράτη- μέλη επεδίωξαν, χωρίς αποτέλεσμα, από τη θέση του προεδρεύοντος στο Συμβούλιο της Ένωσης να καταλήξουν στο κείμενο εκείνο του Κανονισμού, το οποίο θα στάθμιζε κατά τον καλύτερο δυνατό τρόπο τα συμφέροντα όλων των εμπλεκόμενων μερών και θα μπορούσε να αποτελέσει το προς ψήφιση κείμενο από το Ευρωπαϊκό Κοινοβούλιο.

Εντέλει, το σχέδιο το οποίο έγινε δεκτό από το Συμβούλιο είναι αυτό το οποίο εκδόθηκε στις 10 Φεβρουαρίου 2021. Επομένως, ύστερα από περίπου 4 έτη διαβουλεύσεων, άνοιξε ο δρόμος για να εκκινήσει η λεγόμενη διαδικασία «τρίλογος» (trilogue) των θεσμών της Ευρωπαϊκής Ένωσης, ήτοι η Ευρωπαϊκή Επιτροπή, το Συμβούλιο της Ευρωπαϊκής Ένωσης και το Ευρωπαϊκό Κοινοβούλιο, για την οριστικοποίηση του Κανονισμού. Να σημειωθεί δε ότι ο Κανονισμός, σύμφωνα με τον αρχικό προγραμματισμό, θα έπρεπε να έχει τεθεί σε εφαρμογή ταυτογχρόνως με τον ΓΚΠΔ[152], όμως έως και σήμερα δεν έχει γίνει γνωστή καν η ημερομηνία ψήφισής του.

VI. 2. Ποιος είναι ο λόγος της καθυστέρησης υιοθέτησης του Κανονισμού;

Η πραγματικότητα είναι ότι η ψήφιση του Κανονισμού έχει καθυστερήσει υπέρ το δέον, γεγονός που έχει εγείρει πολλά και ποικίλα ερωτήματα. Το βασικότερο εξ αυτών είναι προφανές και συνοψίζεται στις εξής λέξεις: «Γιατί καθυστερεί τόσο πολύ η ψήφιση του Κανονισμού;».

Οι βασικότεροι λόγοι οι οποίοι εντοπίστηκαν είναι δύο. Αρχικά, θα πρέπει να επισημανθεί και πάλι ότι ο υπό μελέτη Κανονισμός αποπειράται να ρυθμίσει, πέραν του πεδίου

---

[151] Η πλήρης και αναλυτική πορεία που έχει έως σήμερα διανύσει ο Κανονισμός εμφαίνεται στην επίσημη ιστοσελίδα της Ευρωπαϊκής Ένωσης: https://eur-lex.europa.eu/procedure/EN/2017_3?qid=1638541574989&rid=502&fbclid=IwAR33gqQ4G02n2ud9pSVHotanl5luLwpwV3yqefQewwWpxXt0H_fafeHETIo

[152] Λ. Κανέλλος, «*The GDPR Handbook*», Νομική Βιβλιοθήκη, 2020, σελ. 120.

που είχε ήδη ρυθμιστεί με την Οδηγία 2002/58/ΕΚ, και ένα πεδίο το οποίο δεν έχει έως σήμερα ρυθμιστεί και αυτό διότι πρόκειται για τεχνολογίες εξαιρετικά καινοτόμες, όπως είναι οι επικοινωνίες μέσω διαδικτύου (Over the Top communication services) και οι επικοινωνίες που πραγματοποιούνται μεταξύ των «έξυπνων συσκευών» (IoT). Ο Κανονισμός, επομένως, θα πρέπει να θεσπίσει μια αρκετά σαφή διάταξη αλλά όχι εξαιρετικά ειδική, αφού αυτό θα στερούσε από τον Κανονισμό τη δυνατότητα να τυγχάνει εφαρμογής σε παρόμοιες τεχνολογίες, οι οποίες πιθανότατα να έχουν αναπτυχθεί όχι σε λίγα χρόνια αλλά ακόμη και μέχρι την ψήφισή του. Ακόμη, και αναφορικά με τη διαφήμιση μέσω διαδικτύου, η οποία ρυθμιζόταν ήδη με την Οδηγία 2002/58/ΕΚ, υπάρχει περίπτωση στο άμεσο μέλλον να αναπτυχθεί κάποια νέα τεχνολογία με την οποία θα λαμβάνει αυτή χώρα, η οποία εν προκειμένω δεν μπορεί να προβλεφθεί και άρα θα εκφεύγει της προστασίας που παρέχει ο Κανονισμός για τους τελικούς χρήστες. Ιδανικά θα πρέπει να αποφευχθεί η υιοθέτηση υπερβολικά ειδικών και περιοριστικών διατάξεων, διότι αυτές πιθανότατα να παρεμποδίζουν την υλοποίηση καινοτόμων επιχειρηματικών ιδεών και σχεδίων[153]. Γίνεται, άρα, αντιληπτό, ότι το τελικό κείμενο του Κανονισμού θα πρέπει να εκδοθεί εφόσον σταθμιστούν όλοι αυτοί οι παράγοντες, γεγονός που δεν καθιστά τη δουλειά των θεσμών της Ένωσης καθόλου εύκολη.

Τέλος, γίνεται εκτενής λόγος για την πίεση που δέχονται οι θεσμοί της Ένωσης από ιδιωτικά συμφέροντα και δη από ισχυρές ομάδες διεθνών εμπορικών και διαφημιστικών συμφερόντων[154], οι οποίες αντέδρασαν από τη δημοσιοποίηση του πρώτου κιόλας σχεδίου του Κανονισμού. Μάλιστα, ήδη στις 10 Ιανουαρίου 2017, η εφημερίδα TheGuardian δημοσίευσε άρθρο με τον τίτλο «*Whatsapp, Facebook and Google face tough new privacy rules under EC proposal*»[155].

Οι κυριότερες εταιρείες που ασκούνε πίεση ενόψει της ψήφισης του Κανονισμού δραστηριοποιούνται στον χώρο της τεχνολογίας και πρόκειται για τους λεγόμενους επιφυείς παρόχους[156] (Over the Top Players). Οι εν λόγω πάροχοι είναι πλέον ευρέως γνωστοί σε όλους μας και αποτελούν κολοσσούς, οι οποίοι αψηφώντας τις παραδοσιακές μεθόδους (καλωδιακές, ασύρματες και δορυφορικές πλατφόρμες), κάνουν χρήση του διαδικτύου ως υποδομή

---

153 https://www.linklaters.com/en/insights/blogs/digilinks/2021/february/eu---the-eprivacy-regulation---let-the-trilogue-begin

154 Λ. Κανέλλος, «*The GDPR Handbook*», Νομική Βιβλιοθήκη, 2020, σελ. 120.

155 W. Gregory Voss, «First the GDPR now the proposed ePrivacy Regulation», Journal of Internet Law, 07/2017, σελίδα 7, διαθέσιμο εδώ: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3008765

156 Επιφυείς πάροχοι ονομάζονται οι υπερατλαντικοί πάροχοι επικοινωνίας και περιεχομένου μέσω διαδικτυακών πρωτοκόλλων.

μετάδοσης περιεχομένου. Ο λόγος γίνεται για εταιρείες που εκμεταλλεύονται εφαρμογές όπως το Viber, το Messenger, το WhatsApp, το Netflix και άλλες παρόμοιες εφαρμογές που έχουμε εντάξει πλήρως στην καθημερινότητά μας, οι οποίες και επιθυμούν με κάθε τρόπο να προστατεύσουν τα εμπορικά και διαφημιστικά συμφέροντά τους, ήτοι τα κέρδη τους, είτε με την κατάργηση του Κανονισμού είτε τουλάχιστον επιφέροντας κάποιες δραστικές εκπτώσεις στο εύρος του και στο πεδίο εφαρμογής του, στον βαθμό που τις επηρεάζει αρνητικά.

Δεν είναι καθόλου τυχαίο το γεγονός ότι στο πλαίσιο των διαπραγματεύσεων για την τελική υιοθέτηση του Κανονισμού κατεγράφη μια από τις μεγαλύτερες καμπάνιες lobbying από τεχνολογικούς κολοσσούς και εκπροσώπους της ψηφιακής βιομηχανίας, η οποία και κατέχει πλέον βασική θέση στην παγκόσμια οικονομία[157].

[157] https://lawyermagazine.gr/the-eprivacy-saga-to-xroniko-gia-thn-psifisi-enos-kanonismou/

VII. ΑΝΤΙ ΕΠΙΛΟΓΟΥ

Από όσα αναφέρθηκαν ανωτέρω, καταλήγουμε στο συμπέρασμα ότι η ψήφιση του Κανονισμού ePrivacy θα συντελέσει στην ειδικότερη, πιο στοχευμένη και ως εκ τούτου αποτελεσματικότερη προστασία των τελικών χρηστών, είτε αυτοί είναι φυσικά είτε νομικά πρόσωπα, αναφορικά με τα δεδομένα των ηλεκτρονικών επικοινωνιών που πραγματοποιούν, με τις πληροφορίες που εντοπίζονται στον τερματικό τους εξοπλισμό, με τα δεδομένα τους που εντάσσονται σε καταλόγους διαθέσιμους στο κοινό και με τα δεδομένα τους που χρησιμοποιούνται από τους παρόχους για διαφημιστικούς σκοπούς και της ιδιωτικότητάς τους εν γένει, στο πλαίσιο των ηλεκτρονικών επικοινωνιών, την οποία πλέον δεν δύναται να παρέχει η υπό κατάργηση οδηγία 2002/58/ΕΚ.

Ο Κανονισμός θεσπίζει σημαντικότατες διατάξεις και ρυθμίζει ζητήματα τα οποία δεν εντοπίζονται σε κανένα άλλο νομοθετικό κείμενο, όπως είναι για παράδειγμα οι επικοινωνίες που λαμβάνουν χώρα μέσω διαδικτύου. Έως την ψήφιση του Κανονισμού και τη θέση του σε εφαρμογή τέτοιου είδους θέματα δεν ρυθμίζονται με ενιαίο τρόπο, παρά μόνο τυγχάνουν εφαρμογής νόμοι και άρθρα αναλογικά, γεγονός που τις περισσότερες φορές δυσχεραίνει τη θέση της εκάστοτε Αρχής ή δικαστικής εξουσίας να κρίνει και να αποδώσει δικαιοσύνη. Δεν θα πρέπει να λησμονούμε ότι η ιδιωτικότητα, με τη ραγδαία εξέλιξη της τεχνολογίας, βρίσκεται στον μεγαλύτερο κίνδυνο, στον οποίο υπήρξε ποτέ, τουλάχιστον έως σήμερα.

Γίνεται, επίσης, σαφές ότι ο Κανονισμός αυτός αποτελεί «αγκάθι» για τους τεχνολογικούς κολοσσούς, παρά το γεγονός ότι επελέχθη από την Επιτροπή η «μέτρια ενίσχυση», καθώς είναι αυτοί οι οποίοι βασίζουν την οικονομική τους δραστηριότητα, κατά κύριο λόγο και σχεδόν εξ ολοκλήρου, στα δεδομένα και στις πληροφορίες που αντλούν από τους τελικούς χρήστες με κύριο στόχο τους τη διαφήμιση προϊόντων και υπηρεσιών, η οποία είναι και αυτή που τους αποφέρει τα συγκλονιστικά ποσά που γίνονται γνωστά ανά διαστήματα. Άλλωστε, όπως συχνά λέγεται «τα δεδομένα είναι το νέο πετρέλαιο» και δυστυχώς τόσο το πετρέλαιο, όσο και τα δεδομένα βρίσκονται στα χέρια των λίγων και ισχυρών, οι οποίοι πασχίζουν να διατηρήσουν τα υπέρογκα κέρδη που αυτά τους αποφέρουν.

Συμπερασματικά, οι θεσμοί της Ένωσης θα πρέπει να προχωρήσουν άμεσα στην ψήφιση και εφαρμογή συνεκτικά και ενιαία του Κανονισμού, να λάβουν υπόψη ζητήματα που θέσανε υπόψη τους τα αρμόδια όργανα με γνωμοδοτήσεις τους και να θέσουν σε πρώτη θέση τα θεμελιώδη δικαιώματα των τελικών χρηστών και όχι τα συμφέροντα των τεχνολογικών

κολοσσών, γεγονός που θα επεκτείνει έτι περαιτέρω τη «δύναμή» τους, σε μια εποχή που ήδη μπορεί να λεχθεί ότι «κυβερνούν τον πλανήτη».

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

- Λ. Κανέλλος, «*The GDPR Handbook*», Νομική Βιβλιοθήκη, 2020.
- Γ. Γιαννόπουλος, «*Εισαγωγή στη Νομική Πληροφορική*», Νομική Βιβλιοθήκη, 2018.
- Κ. Αρκουλή, «*Προστασία Προσωπικών Δεδομένων στις Ηλεκτρονικές Επικοινωνίες*», Νομική Βιβλιοθήκη, 2010.
- Ιωάν. Δημ. Ιγγλεζάκης «*Δίκαιο Πληροφορικής*», Εκδόσεις Σάκκουλα, 2018.
- Γ. Ζέκος, «*Διαδίκτυο, Η/Υ & Τηλεπικοινωνίες στο Ελληνικό Δίκαιο*», Εκδόσεις Σάκκουλα, 2017.
- Ε. Μαργαρίτης «*Προσωπικά Δεδομένα & Προστασία Καταναλωτή*», Νομική Βιβλιοθήκη, 2020.
- Α. Κουσουνή- Πανταζοπούλου, «*Cloud Computing & Νομικά ζητήματα*», Νομική Βιβλιοθήκη, 2022.

Ελληνική Αρθρογραφία

- Χ. Ακριβοπούλου, «*Το δικαίωμα στην προστασία των προσωπικών δεδομένων μέσα από το φακό του δικαιώματος στην ιδιωτική ζωή*», Νομική Βιβλιοθήκη, ΘΠΔΔ, 7/2011.
- Γρ. Τσόλιας, «*Τα τηλεπικοινωνιακά δεδομένα υπό το πρίσμα του απορρήτου: προβληματισμοί εν όψει της ενσωμάτωσης της Οδηγίας 2002/58/ΕΚ*», ΔiΜΕΕ, 2004.
- Β. Μπαντή- Μαρκούτη, Αν. Ματσούκα, Μ. Ηλιοπούλου, Τζ. Κιούση «*Μεταδεδομένα και ηλεκτρονικές επικοινωνίας: Η κατάργηση της Οδηγίας 2006/24/ΕΚ και η USA Freedom Act 2015*», ΔiΜΕΕ, Νομική Βιβλιοθήκη, 3/2015.
- Γρ. Τσόλιας, «*Εξελίξεις στον τομέα της επιτήρησης των ηλεκτρονικών επικοινωνιών: από την Ασφάλεια στην Ελευθερία και τη διεύρυνση της προστατευόμενης επικοινωνίας*», Ποινική Δικαιοσύνη, Νομική Βιβλιοθήκη, Τευχ. 8- 9, Αύγουστος- Σεπτέμβριος, 2017.
- Γρ. Τσόλιας, «*Σημείωμα στην συνεκδ. Υποθ. ΔΕΕ C-203/15 και C-689/15, απόφ. της 21.12.2016- Υποχρεωτική διατήρηση δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών*», ΔΙΜΕΕ, 1/2017.
- Π. Κίτσος, Π. Παππά «*Ενίσχυση της πληροφόρησης και της διαφάνειας στις υπηρεσίες ηλεκτρονικών επικοινωνιών, υπό το πρίσμα της Οδηγίας 2009/136/ΕΚ*», ΔΙΤΕ, 2/2010.
- Αικ. Παπανικολάου, «*Περιορισμοί στο δικαίωμα της ελεύθερης, απόρρητης επικοινωνίας: επίκαιρες σκέψεις για ένα διαχρονικό δίλημμα*», 2020.
- Γ. Τσόλιας, «*Η ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας σύμφωνα με τον Ν 3674/2008 (Παρουσίαση και ερμηνευτική προσέγγιση των διατάξεων)*», Νομική Βιβλιοθήκη, ΔiΜΕΕ, 3/2008.
- Αικ. Παπανικολάου, «*Ανησυχία από το νέο καθεστώς άρσης απορρήτου*», Εφημερίδα «ΤΑ ΝΕΑ», 16 Δεκέμβριου 2019.
- Γρ. Τσόλιας, «*Η προστασία του απορρήτου των επικοινωνιών κατά το ΠΔ 47/2005 (Βασικά χαρακτηριστικά και σύντομη ερμηνευτική προσέγγιση)*», Νομική Βιβλιοθήκη, ΔΙΤΕ, 2/2005.
- Γρ. Τσόλιας, «*Σημείωμα στην ΣτΕ 1593/2016- Η υπαγωγή των εξωτερικών στοιχείων της επικοινωνίας στην διαδικασία άρσης του απορρήτου και η διασφάλισή της από τους Παρόχους*», ΔiΜΕΕ, 4/2016.
- Β. Καρκατζούνης, «*Google Analytics και προστασία προσωπικών δεδομένων Το ψήφισμα της Συνόδου των Εποπτικών αρχών προστασίας προσωπικών δεδομένων της Γερμανίας (Datenschutzkonferenz της 12.5.2020)*», Επιθεώρηση Δικαίου Πληροφορικής, Τ. 1, 2020.

- Β. Καρκατζούνης, «*Cookies και προστασία δεδομένων προσωπικού χαρακτήρα*», ΔΙΤΕ, 2/2019.
- Ε. Μαργαρίτης, «*GDPR και προώθηση προϊόντων μέσω Viber – Σκέψεις με αφορμή την απόφαση 66/2018 της ΑΠΔΠΧ*», Νομική Βιβλιοθήκη, ΔiΜΕΕ, 2/2019.
- Μ. Σκόνδρα, «*Σημείωμα στην ΕιρΑμαρ 129/2019 (Ειδ) – Αζήτητη επικοινωνία για σκοπούς εμπορικής προώθησης και ελάχιστη αποζημίωση του Ν. 3471/2006*», Νομική Βιβλιοθήκη, ΔiΜΕΕ, 3/2019.

Ξενόγλωσση Αρθρογραφία

- W. Gregory Voss, «First the GDPR now the proposed ePrivacy Regulation», Journal of Internet Law, 07/2017
- Samuel Warren και Louis Brandeis, «*The Right to Privacy*», Harvard Law Review, Vol. 4, No 5 (Dec. 15, 1890), pp. 193- 220

Ιστοσελίδες

- Έκθεση Πεπραγμένων ΑΔΑΕ για το έτος 2020, διαθέσιμη εδώ: http://www.adae.gr/fileadmin/docs/pepragmena/2020/EKTHESI_2020.pdf
- Αποψη του Προέδρου και των δύο μελών της ΑΔΑΕ σε σχέση με τα προβλήματα συμβατότητας της πρόσφατης διάταξης του άρθρου 87 του Ν. 4790/2021 με υπέρτερης τυπικής ισχύος κανόνες δικαίου, διαθέσιμη εδώ: https://www.lawspot.gr/nomika-nea/aporrito-epikoinonion-antithesi-toy-arthroy-87-n-4790-2021-pros-tis-eggyiseis-tis
- Ορισμός cookies από την ΑΠΔΠΧ: https://www.dpa.gr/index.php/el/cookies/plirofories/whatis_cookies
- Τηλεφωνικές κλήσεις με ανθρώπινη παρέμβαση από την ΑΠΔΠΧ https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/proothisiproiontwn/thlefwnikes_kliseis_proothisi
- https://www.linklaters.com/en/insights/blogs/digilinks/2021/february/eu---the-eprivacy-regulation---let-the-trilogue-begin

Νομοθετικά Κείμενα

- Κανονισμός ePrivacy, σχέδιο 10.01.2021, διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
- Κανονισμός ΓΚΠΔ, διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679
- Κανονισμός ePrivacy, σχέδιο 10.01.2021, διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017PC0010&from=EN
- Οδηγία 95/46/ΕΚ, διαθέσιμη ηλεκτρονικά εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL
- Οδηγία 2002/58/ΕΚ, διαθέσιμη ηλεκτρονικά εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32002L0058
- Οδηγία 2009/136/ΕΚ, διαθέσιμη ηλεκτρονικά εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0136&from=EL
- Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, διαθέδιμος εδώ: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/charter/pdf/text_el.pdf
- Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, διαθέσιμη εδώ: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.echr.coe.int/documents/convention_ell.pdf
- Οδηγία 2006/24/ΕΚ, διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32006L0024&from=GA
- Κανονισμός 1211/2009/ΕΚ, διαθέσιμος ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009R1211&from=EL.
- Οδηγία 2009/136/ΕΚ, διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0136&from=EL
- Οδηγία 2009/140/ΕΚ διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32009L0140&from=EL.
- Κανονισμός 611/2013/ΕΕ διαθέσιμος ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32013R0611&from=LV
- Οδηγία 2016/1148/ΕΕ διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=EL
- Σύνταγμα του 1844.
- Ισχύον Σύνταγμα.
- Ισχύων Ποινικός Κώδικας.
- Ν. 1291/1982.
- Ν. 3674/2008.
- Ν. 4619/2019.
- Ν. 3471/2006.
- Ν. 2225/1994.
- ΠΔ 47/2005.
- Ν. 4790/2021.
- Ν. 4640/2019.
- Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000.
- Από 18.09.2019 Σχέδιο του Κανονισμού ePrivacy.
- Από 04.10.2019 Σχέδιο του Κανονισμού ePrivacy.
- Από 08.11.2019 Σχέδιο του Κανονισμού ePrivacy.
- Κανονισμός (ΕΕ) 182/2011 διαθέσιμος εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32011R0182&from=BG

Νομολογία

- Digital Rights Ireland Ltd. κατά Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform και λοιπών. Διαθέσιμη ηλεκτρονικά: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62012CJ0293&from=el
- Απόφαση του ΔΕΕ επί της υπόθεσης με αριθμό C-140/20 διαθέσιμη: https://curia.europa.eu/juris/document/document.jsf;jsessionid=DBB9D8ADC8D3EAAD57BFEE382A5B783D?text=&docid=257242&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=5042309)
- Απόφαση ΑΠ 711/2011.
- Απόφαση ΑΠ 203/2014.
- Απόφαση ΣτΕ με αριθμό 1593/2016 απόφαση του Δ' τμήματός εδώ: http://www.adjustice.gr/webcenter/portal/ste/ypiresies/nomologies?_afrLoop=33866166662155739#!%40%40%3F_afrLoop%3D33866166662155739%26centerWidth%3D65%2525%26leftWidth%3D0%2525%26npath%3D%252Fwebcenter%252Fportal%252Fste%252Fypiresies%252Fnomologies%26rigthWidth%3D35%2525%26showFooter%3Dfalse%26showHeader%3Dtrue%26_adf.ctrl-state%3Dkj8fgltcw_29
- Απόφαση 570/2006 ΑΠ.
- Απόφαση 711/2011 ΑΠ.

- Απόφαση 689/2014 ΑΠ.
- Υποθέσεις C-203/15 και C-698/15 (Tele2 Sverige AB κατά Post-och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis) διαθέσιμη η απόφαση εδώ: https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EL
- Υπόθεση Malone κατά Ηνωμένου Βασιλείου (1984).
- Απόφαση ΑΠΔΠΧ με αριθμό 66/2018.
- Απόφαση Μονομελούς Πρωτοδικείου Αθηνών με αριθμό 227/2022.

Γνώμες και Γνωμοδοτήσεις

- Γνωμοδότηση 06.2017 του Ευρωπαικού Επόπτη Προσωπικών Δεδομένων διαθέσιμη εδώ: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf
- Δήλωση 03.2021 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ), διαθέσιμη εδώ: https://edpb.europa.eu/system/files/2021-06/edpb_statement_032021_eprivacy_regulation_el.pdf
- Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής, διαθέσιμη εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017AE0655&from=EN
- Report on OTT Services, διαθέσιμο εδώ: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services
- Γνωμοδότηση του ΑΠ με αριθμό 9/2009 εδώ: https://eisap.gr/%ce%b3%ce%bd%cf%89%ce%bc%ce%bf%ce%b4%cf%8c%cf%84%ce%b7%cf%83%ce%b7-09-2009/
- Γνωμοδότηση Ι. Τέντε, με αριθμό 12/2009.
- Γνωμοδότηση Α. Κατσιδώρης με αριθμό 09/2011.
- 1/2005 Γνωμοδότηση της ΑΔΑΕ.

Διπλωματικές Εργασίες

- Αικ. Μαστοροστέργιου, «*Η παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας & της προφορικής συνομιλίας κατ' άρθρο 370Α Π.Κ.*», Διπλωματική Εργασία στο πλαίσιο του Διαπανεπιστημιακού Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο & Πληροφορική», Φεβρουάριος 2021.
- Π. Κίτσος, «*Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών. Ενσωμάτωση των ρυθμίσεων της Ευρωπαϊκής Ένωσης στο ελληνικό δίκαιο*», Διδακτορική Διατριβή στο Πανεπιστήμιο Μακεδονίας Οικονομικών και Κοινωνικών Επιστημών, Τμήμα Εφαρμοσμένης Πληροφορικής, Θεσσαλονίκη 2011, διαθέσιμη εδώ: https://dspace.lib.uom.gr/bitstream/2159/14739/2/Kitsos_Phd2011.pdf