

ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES



ΣΧΟΛΗ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ, ΕΥΡΩΠΑΪΚΩΝ ΚΑΙ ΠΕΡΙΦΕΡΕΙΑΚΩΝ ΣΠΟΥΔΩΝ
Στο ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΔΙΕΘΝΕΣ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ»
ΚΑΤΕΥΘΥΝΣΗ: ΕΥΡΩΠΑΪΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ

«Ζητήματα ποινικής προστασίας των προσωπικών δεδομένων κατά τη χρήση ηλεκτρονικών μέσων επικοινωνίας και μετάδοσης δεδομένων στο χώρο της εργασίας υπό το φως της Ευρωπαϊκής Δικαιοταξίας»

"Issues of criminal protection of personal data during usage of electronic means of communication and data transmission in the workplace from the perspective of European legislation"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Θεολόγος Δελλήβεης- Δομένικος

Αθήνα, 2023

Τριμελής Επιτροπή

Όλγα Τσόλκα, Καθηγήτρια Παντείου Πανεπιστημίου (Επιβλέπουσα)

Βασίλειος Χατζόπουλος, Καθηγητής Παντείου Πανεπιστημίου

Νικόλαος Λίβος, Επίκουρος Καθηγητής ΕΚΠΑ



Copyright © Θεολόγος Δελλήβης – Δομένικος, 2023

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνώμων του συγγραφέα.

Στη σύζυγό μου Μυρσίνη

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ.....	5
SUMMARY	6
ΠΡΟΛΟΓΟΣ.....	7
ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ.....	9
ΤΟ ΙΣΧΥΟΝ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ	9
ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ	13
ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΡΓΑΖΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΕΣΩΤΕΡΙΚΩΝ ΕΡΕΥΝΩΝ	13
I. ΕΙΣΑΓΩΓΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ	13
II. ΈΝΝΟΙΑ ΚΑΙ ΑΡΧΕΣ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΡΓΑΖΟΜΕΝΩΝ	13
III. ΈΝΝΟΙΑ ΚΑΙ ΦΥΣΙΟΓΝΩΜΙΑ ΤΩΝ ΕΣΩΤΕΡΙΚΩΝ ΕΡΕΥΝΩΝ	22
ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ.....	27
ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ ΚΑΙ ΠΟΙΝΙΚΗΣ ΕΥΘΥΝΗΣ	27
I. ΕΙΣΑΓΩΓΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ	27
II. Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΗΣ ΖΩΗΣ ΤΟΥ ΕΡΓΑΖΟΜΕΝΟΥ	28
III. ΌΡΟΙ ΚΑΙ ΠΡΟΫΠΟΘΕΣΕΙΣ ΓΙΑ ΤΟΝ ΕΛΕΓΧΟ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ ΣΤΟ ΧΩΡΟ ΕΡΓΑΣΙΑΣ ΤΟΥΣ	31
IV. ΠΟΙΝΙΚΗ ΕΥΘΥΝΗ ΕΡΓΟΔΟΤΗ ΚΑΤΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΟΥ ΕΡΓΑΖΟΜΕΝΟΥ ΣΤΟ ΠΛΑΙΣΙΟ ΕΣΩΤΕΡΙΚΩΝ ΕΡΕΥΝΩΝ	39
V. ΠΟΙΝΙΚΗ ΕΥΘΥΝΗ ΕΡΓΑΖΟΜΕΝΟΥ ΚΑΤΑ ΤΗ ΧΡΗΣΗ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΕΣΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ ..	46
ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΣΚΕΨΕΙΣ	48
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	49

Περίληψη

Στην παρούσα διπλωματική εργασία αναπτύσσεται το νομοθετικό πλαίσιο προστασίας των προσωπικών δεδομένων σε επίπεδο ενωσιακού και εσωτερικού δικαίου, με αναφορά κυρίως στις ρυθμίσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (Κανονισμού 2016/679) και του Ν.4524/2019. Επίσης γίνεται αναφορά στις νομολογιακές γραμμές που έχουν χαραχθεί από τα Ευρωπαϊκά Δικαστήρια στο πεδίο της προστασίας των προσωπικών δεδομένων και του απορρήτου των επικοινωνιών. Τέλος γίνεται αναφορά στις απόψεις που έχουν υποστηριχθεί στη γερμανική και ελληνική θεωρία σε συνάρτηση με το ζήτημα της επεξεργασίας από τον εργοδότη των δεδομένων ηλεκτρονικής αλληλογραφίας και περιήγησης του εργαζομένου στο διαδίκτυο.

Τα συμπεράσματα της εργασίας συνοψίζονται στα εξής: Ανεξαρτήτως της γραμμής που ο εκάστοτε εργοδότης τηρεί ως προς το δικαίωμα χρήσης από τους εργαζομένους των ηλεκτρονικών μέσων επικοινωνίας της επιχείρησης (για υπηρεσιακούς σκοπούς αποκλειστικά ή όχι), ουδόλως υποχωρεί η υποχρέωσή του για προστασία της προσωπικότητας του εργαζόμενου, στην οποία εντάσσεται και η προστασία των προσωπικών δεδομένων του. Ωστόσο, λόγοι που συνέχονται με την επιχειρηματική ελευθερία του εργοδότη και την διαφύλαξη των δικαιωμάτων αυτού, επιβάλλουν τη διενέργεια εσωτερικών ερευνών. Μεταξύ των διερευνητικών μέτρων που επιστρατεύονται είναι η επεξεργασία ηλεκτρονικών δεδομένων των εργαζομένων, τα οποία, πέραν του προσωπικού χαρακτήρα τους, ενίοτε εμπίπτουν και στο προστατευτικό πεδίο του τηλεπικοινωνιακού απορρήτου. Κατά την εν λόγω επεξεργασία πρέπει να τηρούνται απαρέγκλιτα οι όροι και οι αρχές που τίθενται για την προστασία των προσωπικών δεδομένων από τον Γ.Κ.Π.Δ. και το Ν.4624/2019. Σε περίπτωση μη συμμόρφωσης του εργοδότη, γεννιούνται ποινικές ευθύνες για παραβίαση του τηλεπικοινωνιακού απορρήτου και των προσωπικών δεδομένων. Ποινικές ευθύνες γεννιούνται ωστόσο και στο πρόσωπο του εργαζομένου, ιδίως όταν, παραγνωρίζοντας όρους που έχουν τεθεί από τον εργοδότη για τη χρήση των ηλεκτρονικών μέσων μιας εταιρείας, υποπίπτει σε συμπεριφορές, οι οποίες ενέχουν ποινικά στοιχεία και μπορούν να θέσουν σε κίνδυνο την οικονομική και νομική υπόσταση της επιχείρησης.

Summary

In the current thesis we present the legislative framework for the protection of personal data at the level of the European Union and domestic law, with reference mainly to the provisions of the General Data Protection Regulation (Regulation 2016/679) and the Law 4524/2019. Reference is also made to the jurisprudential principles established by the European Courts in the field of personal data protection and privacy of communications. Lastly, reference is made to the opinions that have been supported in German and Greek theory in connection with the matter of the processing made by the employer of the employee's e-mail and internet browsing data.

The conclusions of this thesis are summarised as follows: Regardless of the employer's policy regarding the employees' right to use the company's electronic means of communication (for official purposes only or not), the employer's obligation to protect the employee's personality, which includes the protection of personal data, does not retreat in any case. However, reasons associated with the employer's freedom to conduct his business and the safeguarding of his rights require internal investigations to be conducted. Among these investigative measures is the processing of employees' electronic data which, beyond their personal nature, may also fall within the scope of the protection of privacy of communications. During such a processing, the conditions and principles set by the GDPR and Law 4624/2019 for the protection of personal data must be strictly followed. In case of non-compliance by the employer, criminal liability for breach of telecommunication privacy and personal data is born. However, criminal liability also arises for the employee, especially when, by disregarding any terms set by the employer for the use of the company's electronic means, the employee engages in conduct that involves criminal offences and may jeopardise the financial and legal status of the company.

Πρόλογος

Αφορμή για τη συγγραφή της παρούσας διπλωματικής αποτέλεσε η ραγδαία αύξηση και διάδοση της χρήσης των ηλεκτρονικών μέσων επικοινωνίας που έλαβαν χώρα, κατά τα τελευταία χρόνια, στις εργασιακές σχέσεις τόσο του δημοσίου όσο και του ιδιωτικού τομέα. Είναι γεγονός ότι στην Ελλάδα, όπου η χρήση των πληροφοριακών συστημάτων στον εργασιακό χώρο δεν ήταν τόσο διαδεδομένη, οι εξελίξεις υπήρξαν ακόμα πιο ραγδαίες και σε μεγάλο βαθμό υπαγορεύθηκαν από τις ιδιαίτερες συνθήκες που δημιούργησε η πανδημική κρίση του κορωνοϊού. Σύμφωνα με επίσημα στοιχεία κατά το αρχικό κύμα αντιμετώπισης της ως άνω κρίσης αυξήθηκε η παροχή εξ αποστάσεως εργασίας πάνω από το 1/3 (37%) των εργαζομένων στην Ε.Ε, οι οποίοι, ενώ έως τότε απασχολούνταν δια ζώσης στο χώρο εργασίας τους, πλέον εντάχθηκαν σε καθεστώς τηλεργασίας, ενώ το ποσοστό αυτό στην Ελλάδα ανήλθε στο 26,2%¹. Επιπλέον, το καλοκαίρι του έτους 2021 η εκτίμηση για την Ελλάδα ως προς την παροχή εργασίας εξ αποστάσεως των εργαζομένων μισθωτών άγγιζε το 40%², ενώ βάσει πρόσφατης μελέτης³ έως και το 25% των συνολικά απασχολούμενων (μισθωτών και αυτοαπασχολούμενων, περί τους 500.000 εργαζομένους) θα μπορούσε να ενταχθεί σε καθεστώς πλήρους τηλεργασίας⁴. Μάλιστα ήταν τόσο μεγάλες οι ανακατατάξεις που επήλθαν στον εργασιακό χώρο λόγω του κορωνοϊού, οι οποίες, χωρίς υπερβολή, μπορεί να λεχθεί ότι άλλαξαν τη νοοτροπία που μέχρι τότε επικρατούσε κυρίως στις δημοσιοϋπαλληλικές σχέσεις και αποτέλεσαν αφορμή για τον εκσυγχρονισμό εργασιακών τομέων (όπως π.χ. δικαστηρίων ή φορέων εξυπηρέτησης πολιτών), που μέχρι τότε λειτουργούσαν με πιο παραδοσιακές μεθόδους.

Η ολοένα αυξανόμενη εισχώρηση των ηλεκτρονικών μέσων επικοινωνίας και διαδικτυακής περιήγησης στο χώρο της εργασίας καθιστά επίκαιρο το ζήτημα της προστασίας των προσωπικών δεδομένων του εργαζόμενου και της διαφύλαξης του απορρήτου των επικοινωνιών του. Το πεδίο των εργασιακών σχέσεων είναι, ίσως, το

¹ Πηγή Eurofound 2020, <https://www.eurofound.europa.eu/data/covid-19/working-teleworking>

² Sostero M, S Milasi, J Hurley, E Fernandez-Macias and M Bisello (2020), "Teleworkability and the COVID-19 crisis: a new digital divide?" JRC Working Papers Series on Labour, Education and Technology 2020/05, European Commission.

³ Pouliakas, 2020. "Working at Home in Greece: Unexplored Potential at Times of Social Distancing?," IZA Discussion Papers 13408, Institute of Labor Economics (IZA). <http://ftp.iza.org/dp13408.pdf>.

⁴ Αναλυτικά στοιχεία για την τηλεργασία στην Ε.Ε. πριν και μετά την πανδημία λόγω κορωνοϊού μπορούν να αναζητηθούν στο Θεματικό Δελτίο ενημέρωσης Νο3 Νοεμβρίου 2020 του Εθνικού Ινστιτούτου Εργασίας και Ανθρώπινου Δυναμικού https://www.eiead.gr/publications/docs/EIEAD_THEMATIC_ISSUE_TELEWORK_FINAL.pdf

μοναδικό, όπου, από τη φύση της η εισαγωγή της πληροφορικής και των νέων τεχνολογικών μεθόδων άσκησης του διευθυντικού δικαιώματος δημιουργεί διακινδυνεύσεις για τα ατομικά δικαιώματα από αθέμιτες επεξεργασίες προσωπικών δεδομένων του εργαζομένου, ποιοτικά και ποσοτικά, με πολύ μεγαλύτερη ένταση απ' ό,τι σε άλλα πεδία επαγγελματικής και κοινωνικής δραστηριότητας⁵. Οι νέες τεχνολογίες πληροφορικής και επικοινωνιών επιτρέπουν οι συλλεγόμενες πληροφορίες να είναι λεπτομερέστερες και πληρέστερες, να καλύπτουν δεδομένα συμπεριφοράς και χαρακτήρα, παρέχοντας έτσι στον εργοδότη την δυνατότητα «κατάρτισης του προφίλ» του εργαζομένου⁶. Η αξιολόγηση του εργαζομένου αποκλειστικά μέσω μιας αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων του, χωρίς δηλαδή την ανθρώπινη παρέμβαση, ενέχει για τον εργαζόμενο σοβαρούς κινδύνους, για την αντιμετώπιση των οποίων προβλέπονται συγκεκριμένες προστατευτικές εγγυήσεις⁷.

⁵ Βλ. Ζερδελή, Εργατ. Δικ., σελ. 976, 76· Θεοδόση, Βασικές αρχές προστασίας των προσωπικών δεδομένων των εργαζομένων, ΔΕΕ 2006, 592· Κουκιάδη, Εργατ.Δικ., σελ. 835· Λαδά, Το δικαίωμα της προσωπικότητας του εργαζομένου, σελ. 81 επ., 315 επ· Δούκα, Η προστασία των προσωπικών δεδομένων στη σχέση εργασίας, σελ. 18 επ.

⁶ Βλ. άρθρο 4 στοιχ. 4 του Κανονισμού 2016/679 (Γενικού Κανονισμού για την προστασία δεδομένων) σύμφωνα με το οποίο ως κατάρτιση προφίλ ορίζεται «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίστανται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου».

⁷ Βλ. άρθρα 22 Κανονισμού 2016/679.

Κεφάλαιο πρώτο

Το ισχύον νομοθετικό πλαίσιο

Η προστασία προσωπικών δεδομένων είναι εκδήλωση του δικαιώματος πληροφοριακής αυτοδιάθεσης ή, κατ' άλλη διατύπωση, του πληροφοριακού αυτοπροσδιορισμού, του δικαιώματος δηλαδή κάθε φυσικού προσώπου να αποφασίζει το ίδιο για την αποκάλυψη, διάθεση και χρησιμοποίηση προσωπικών του δεδομένων. Το δικαίωμα αυτό, ειδικότερη εκδήλωση του γενικού δικαιώματος της προσωπικότητας (άρθρ. 5 παρ.1 Συντ.) και του δικαιώματος στην ιδιωτική ζωή (άρθρ. 9), με την αναθεώρηση του Συντάγματος του 2001 κατοχυρώθηκε σε ρητή συνταγματική διάταξη (άρθρ. 9^Α). Η εισαγωγή ειδικής συνταγματικής διάταξης δηλώνει και ταυτόχρονα αναγνωρίζει την ιδιαίτερη αξία του δικαιώματος, δηλαδή την σημασία που έχει η χρήση προσωπικών δεδομένων για τις προϋποθέσεις προστασίας, ανάπτυξης και αυτόνομης δράσης ενός προσώπου μέσα σε μία κοινωνία, κύριο χαρακτηριστικό της οποίας είναι η ραγδαία τεχνολογική ανάπτυξη⁸. Αυτές οι συνταγματικές διατάξεις πρέπει να λαμβάνονται υπόψη κατά την προστασία των δεδομένων του εργαζομένου υπέρ αυτού ως προσώπου που επηρεάζεται από την επεξεργασία δεδομένων. Από την άλλη πλευρά, υπάρχουν επίσης συνταγματικές εγγυήσεις υπέρ του εργοδότη, ιδίως η οικονομική ελευθερία (άρθρ. 5 παρ. 1 Συντ.) και η ιδιοκτησία (άρθρ. 17 Συντ.). Τα αντικρουόμενα δικαιώματα και συμφέροντα πρέπει να εξισορροπούνται όσο το δυνατόν πιο ήπια μέσω πρακτικών σταθμίσεων.

Πέραν των ανωτέρω συνταγματικών επιταγών, η νομοθεσία περί προστασίας δεδομένων πρέπει να ερμηνεύεται, ταυτόχρονα και κατά προτεραιότητα, σύμφωνα με τις νομικές επιταγές της Ευρωπαϊκής Ένωσης. Σε επίπεδο πρωτογενούς δικαίου, θα πρέπει να αναφερθεί το θεμελιώδες δικαίωμα στην προστασία των προσωπικών δεδομένων (άρθρ. 8 ΧΘΔΕΕ, άρθρ. 16 ΣΛΕΕ).⁹ Αυτό συμπληρώνεται από το επικουρικό δικαίωμα σεβασμού της ιδιωτικής ζωής σύμφωνα με το άρθρο 7 ΧΔΘΕΕ.¹⁰ Το άρθρο 7 ΧΔΘΕΕ εμπεριέχει την ελευθερία επικοινωνίας ως περαιτέρω θεμελιώδες δικαίωμα υπέρ του ενδιαφερόμενου, το οποίο μπορεί να συγκριθεί με το απόρρητο των τηλεπικοινωνιών του άρθρου 19 παρ. 1 Συντ. Από την πλευρά του, ο εργοδότης μπορεί

⁸ Βλ. Μήτρου σε: Σύνταγμα, κατ' άρθρον ερμηνεία, σελ. 217.

⁹ Βλ. Σαρμά, σε: Σαγκπεκίδου/Ταγαρά, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, 2020, σελ. 103 επ.

¹⁰ Βλ. Τάκη, σε: Σαγκπεκίδου/Ταγαρά, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, 2020, σελ. 86 επ.

να επικαλεστεί την προστασία της επιχειρηματικής του ελευθερίας (άρθρο 16 ΧΘΔΕΕ)¹¹ και του δικαιώματος ιδιοκτησίας του (άρθρο 17 ΧΘΔΕΕ).

Σε επίπεδο δευτερογενούς δικαίου βασικό νομοθετικό κείμενο¹² είναι ο Γενικός Κανονισμός για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (Γ.Κ.Π.Δ.)¹³, ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2016, αντικαθιστώντας την προϊσχύουσα Οδηγία 95/46/Ε.Κ.. Με τη θέσπιση του ως άνω Κανονισμού που ως νομική πράξη παράγει, από τις 25 Μαΐου 2018, άμεση ισχύ στα επιμέρους κράτη μέλη με βάση την αρχή της υπεροχής του δικαίου της Ευρωπαϊκής Ένωσης (αμεσότητα και δεσμευτικότητα)¹⁴, επιχειρήθηκε η μείωση του νομικού κατακερματισμού και η εξασφάλιση μεγαλύτερης ασφάλειας δικαίου μέσω της θέσπισης ενός εναρμονισμένου συνόλου βασικών κανόνων και της βελτίωσης της προστασίας των θεμελιωδών δικαιωμάτων των φυσικών προσώπων στο πλαίσιο μιας εύρυθμης λειτουργίας της εσωτερικής αγοράς. Συγχρόνως όμως ο Κανονισμός διατήρησε σε αρκετές περιπτώσεις την ευελιξία των κρατών μελών με συγκεκριμένες διατάξεις του, με τις οποίες παρέχεται σ' αυτά η ευχέρεια να διατηρούν ή να θεσπίζουν εθνικές διατάξεις τόσο για την ειδική ρύθμιση κάποιων θεμάτων όσο και για τις ανάγκες εφαρμογής του Γ.Κ.Π.Δ.¹⁵.

Τέτοια ευελιξία παρέχει και το άρθρο 88 Γ.Κ.Π.Δ., που αφορά την ευχέρεια για θέσπιση ειδικών κανόνων κατά την επεξεργασία «στο πλαίσιο της απασχόλησης». Έτσι στην επεξεργασία προσωπικών δεδομένων του εργαζόμενου από τον εργοδότη εφαρμόζονται οι διατάξεις του Γ.Κ.Π.Δ. λόγω της γενικής (οριζόντιας) εφαρμογής

¹¹ Για την ερμηνεία του άρθρου 16 ΧΘΔΕΕ βλ. Σαρμά, σε: Σαγκπεκίδου/Ταγαρά, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, 2020, σελ. 86 επ. Συναφώς σημειώνεται ότι η ελευθερία του επαγγέλματος σύμφωνα με το άρθρο 15 ΧΘΔΕΕ δε διαδραματίζει, κατά κανόνα, κάποιον ρόλο, καθώς είτε αφορά μόνο τους μισθωτούς είτε υποχωρεί έναντι του άρθρου 16 ΧΘΔΕΕ όσον αφορά τους αυτοαπασχολούμενους. Βλ. Jarass, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ άρθρο 16 παρ. 4· επίσης Λέντζη, σε: Σαγκπεκίδου/Ταγαρά, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, 2020, σελ. 177-178.

¹² Η θέσπιση του GDPR ήταν ίσως η πιο προσεγμένη, αλλά όχι η μοναδική νομική πράξη. Ο Κανονισμός αποτελεί μέρος ενός πανευρωπαϊκού εκσυγχρονισμού της νομοθεσίας περί προστασίας δεδομένων. Τον Μάιο του 2018, για παράδειγμα, εγκρίθηκε η αναθεωρημένη Σύμβαση 108 του Συμβουλίου της Ευρώπης (Σύμβαση για την Προστασία των Ατόμων σε σχέση με την Αυτόματη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα) (πρβλ.: Πρωτόκολλο τροποποίησης SEV No. 223). Σε επίπεδο ΕΕ, η Οδηγία (ΕΕ) 2016/680 (ΕΕ ΕΕ L 119, σ. 89 επ.) εισήγαγε ρυθμίσεις για την προστασία δεδομένων στον τομέα της ποινικής δικαιοσύνης.

¹³ Κανονισμός 2106/679, ΕΕ ΕΕ L 119, σ. 1 επ.

¹⁴ Αναλυτικά βλ. Σκουρή, Συνθήκη της Λισσαβόνας, ερμηνεία κατ' άρθρον, Σάκκουλας 2020, σελ. 1835 - 1838.

¹⁵ Συνολικά υπάρχουν σχεδόν πενήντα ρήτρες που παρέχουν ευελιξία προς διαμόρφωση νέων κανόνων ή προς προσαρμογή. Λόγω της νομοθετικής αυτής επιλογής επικρίθηκε ο κανονισμός ως «υβρίδιο Κανονισμού» η ως «οδηγία υπό τον μανδύα Κανονισμού». Σχετική ευελιξία των κρατών μελών παρείχε και η οδηγία. Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 978, 81· Λεμπέση, ΔΕΝ 2018, 500.

τους¹⁶ και συμπληρώνονται αφενός από τις ρυθμίσεις του εθνικού δικαίου των κρατών μελών, που εναρμονίζονται με αυτές και αφετέρου από τους ειδικούς κανόνες που τυχόν θεσπίζουν τα κράτη μέλη αξιοποιώντας την ευχέρεια που τους παρέχει το άρθρο 88. Ο Έλληνας νομοθέτης, κάνοντας χρήση της «ρήτρας ανοίγματος», κατ' άρθρο 88 παρ.1 του Γ.Κ.Π.Δ., ψήφισε το Ν.4624/2019 (ΦΕΚ Α 137/29.8.2019), ο οποίος, μεταξύ άλλων, προβαίνει στην αναδιάρθρωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα σε επίπεδο σύνθεσης και αρμοδιοτήτων, ενώ περιέχει και ειδική ρύθμιση (άρθρ. 27) για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των συμβάσεων εργασίας τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα.

Εφόσον ο Γ.Κ.Π.Δ. διατηρεί τους στόχους, τις αρχές, τα δικαιώματα των υποκειμένων και τις υποχρεώσεις των υπευθύνων επεξεργασίας που θέσπιζε η Οδηγία 95/46/Ε.Κ., είναι αξιοποιήσιμη προς ερμηνεία των κανόνων του η νομολογία του Δ.Ε.Ε. επί αυτής, η νομολογία των εθνικών δικαστηρίων σχετικά με την ερμηνεία των διατάξεων των εθνικών νομοθετημάτων (Ν. 2472/1997, Ν. 4264/2019) που ίσχυσαν μέχρι σήμερα, οι αποφάσεις των εθνικών αρχών για την εποπτεία της εφαρμογής της Οδηγίας και δη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (στο εξής Α.Π.Δ.Π.Χ.) στην χώρα μας¹⁷, οι συστάσεις, οι γνώμες και οι οδηγίες της Ομάδας Εργασίας του άρθρου 29¹⁸ και τέλος οι Οδηγίες της Α.Π.Δ.Π.Χ.¹⁹. Εξίσου σημαντική είναι η νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ), το οποίο με σειρά αποφάσεων συνέβαλε στην εξύφανση του νομικού πλαισίου προστασίας των προσωπικών δεδομένων των εργαζομένων, όπως εν πολλοίς ενσωματώθηκε τόσο στον Γ.Κ.Π.Δ. όσο και στον εφαρμοστικό αυτού νόμο 4624/2019.

¹⁶ Μια από τις καινοτομίες του Γ.Κ.Π.Δ. αποτελεί η δέσμευση του «εκτελούντος την επεξεργασία» ομοίως με τον «υπεύθυνο επεξεργασίας», και συνεπώς, όσα ισχύουν για τον εργοδότη ως «υπεύθυνο επεξεργασίας» αφορούν και κάθε τρίτο που ενεργεί ως «εκτελών την επεξεργασία» των προσωπικών δεδομένων των εργαζομένων, όπως είναι οι εταιρείες που ασχολούνται με την διοίκηση προσωπικού ή με την εξαγωγή μισθοδοσίας.

¹⁷ Σημαντική καινοτομία που εισέφερε ο Κανονισμός είναι η κατάργηση της προβλεπόμενης στην Οδηγία και στο Ν.2472/1997 υποχρέωσης γνωστοποίησης της επεξεργασίας προσωπικών δεδομένων στις εποπτικές αρχές, με αποτέλεσμα να ακυρώνεται στην ουσία ο προληπτικός έλεγχος που ασκούσε υπό την ισχύ του Ν.2472/1997 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα μέσω των γνωμοδοτήσεών της, που πρόσφεραν καιρικές λύσεις σε σοβαρά ζητήματα επεξεργασίας των προσωπικών δεδομένων των εργαζομένων.

¹⁸ Βλ. και από την από 82.2017 Γνώμη 2/2017 για την επεξεργασία δεδομένων στην εργασία υπό τον Γ.Κ.Π.Δ., που συμπληρώνει την Γνώμη 8/2001 για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο εργασιακό πλαίσιο και το έγγραφο της 29.5.2002 για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας. Όλα τα κείμενα της Ομάδας Εργασίας του άρθρου 29 βρίσκονται αναρτημένα στην ηλεκτρονική διεύθυνση http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

¹⁹ Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ΕΕργΔ. 2018, σελ. 643.

Εξάλλου πολύ σημαντικός υπήρξε και ο ρόλος των δικαστηρίων των επιμέρους κρατών-μελών της Ευρωπαϊκής Ένωσης, όπως λ.χ. της Γερμανίας και της Ελλάδας, που κλήθηκαν να αποφανθούν για διάφορα ζητήματα προστασίας των προσωπικών δεδομένων των εργαζομένων, ενόψει και των σύγχρονων τεχνολογικών εξελίξεων, οι οποίες, όπως προαναφέρθηκε, επηρεάζουν τόσο τις επιχειρηματικές πρακτικές όσο και τις μορφές παροχής εξαρτημένης εργασίας. Τέλος, παρόλο που στην Ελλάδα είναι σπάνιες οι συλλογικές συμβάσεις εργασίας, οι οποίες ρυθμίζουν ζητήματα προστασίας των προσωπικών δεδομένων των εργαζομένων²⁰, μέσα από τις νέες ρυθμίσεις του Γενικού Κανονισμού Προστασίας Δεδομένων και του Ν. 4624/2019 προσδίδεται η προσήκουσα σημασία στο θεσμό της συλλογικής αυτονομίας, που σε άλλα κράτη έχει αναπτυχθεί σημαντικά και παίζει πρωτεύοντα ρόλο στην προστασία των προσωπικών δεδομένων των εργαζομένων²¹.

Στο πλαίσιο της παρούσας διπλωματικής, κατ' αρχάς γίνεται αναφορά στις αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων των εργαζομένων κατά τη χρήση ηλεκτρονικών μέσων επικοινωνίας και μετάδοσης δεδομένων στο χώρο της εργασίας, όπως αυτές διαμορφώνονται στο πλαίσιο της ως άνω αλληλεπίδρασης μεταξύ κοινοτικού και εσωτερικού δικαίου. Στη συνέχεια αναλύονται τα βασικότερα ζητήματα που ανακύπτουν σε ποινικό επίπεδο και αφορούν τους όρους επεξεργασίας των δεδομένων και διενέργειας εσωτερικών ερευνών από τον εργοδότη καθώς και τις ποινικές ευθύνες που γεννιούνται σε περίπτωση μη τήρησής τους.

²⁰ Ρυθμίσεις γενικού περιεχομένου για την προστασία των προσωπικών δεδομένων των εργαζομένων εντοπίζονται κυρίως σε επίπεδο Εθνικής Γενικής Συλλογικής Σύμβασης Εργασίας, όπου στο άρθρο 17 αναφέρονται τα εξής: «οι συμβαλλόμενες εργοδοτικές οργανώσεις υπογραμμίζουν στα μέλη τους τις υποχρεώσεις που προκύπτουν για τις επιχειρήσεις από το νομοθετικό πλαίσιο, καθόσον αφορά την προστασία του ατόμου σχετικά με θέματα προσωπικού χαρακτήρα που αποσκοπεί στην προστασία της προσωπικότητας των εργαζομένων». Βλ. και Παπαϊωάννου, Ο έλεγχος από τον εργοδότη της ηλεκτρονικής αλληλογραφίας και της ενασχόλησης του μισθωτού με το διαδίκτυο, ΕΕργΔ 2006, σελ. 733.

²¹ Kramer: Betriebsrat und Datenschutz in: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis - Praxishandbuch zum Arbeitnehmerdatenschutz, hrsg. von Stephan Weth, Maximilian Herberger und Michael Wächter, 2014, σελ. 485επ.· Däubler, Internet und Arbeitsrecht, Web 2.0, Social Media und Crowdwork, 2015, σελ. 363επ.

Κεφάλαιο δεύτερο

Επεξεργασία προσωπικών δεδομένων εργαζομένων στο πλαίσιο εσωτερικών ερευνών

I. Εισαγωγικές παρατηρήσεις

Με πλήρη αντίληψη του εύρους της προβληματικής επί του ζητήματος της ποινικής προστασίας προσωπικών δεδομένων στις εργασιακές σχέσεις, το οποίο επ' ουδενί θα μπορούσε να αναπτυχθεί επαρκώς στο πλαίσιο της παρούσας διπλωματικής²², επιχειρείται στη συνέχεια να σκιαγραφηθούν τα βασικότερα σημεία αυτής της προστασίας στην περίπτωση των εσωτερικών ερευνών, οι οποίες, κατά καιρούς διενεργούνται από τον εργοδότη και αφορούν στα δεδομένα που είτε διακινούνται από τους εργαζόμενους μέσω της ηλεκτρονικής αλληλογραφίας, είτε «φορτώνονται» μέσω διαφόρων (επιχειρηματικών και μη) ιστοσελίδων. Η επιλογή δε του συγκεκριμένου επιμέρους ζητήματος υπαγορεύθηκε από το γεγονός ότι οι έρευνες αυτές συνιστούν ίσως την δραστηκότερη επέμβαση²³ του εργοδότη στα προσωπικά δεδομένα των εργαζομένων, οι οποίοι πολλές φορές αγνοούν τα αίτια που προκάλεσαν μία τέτοια έρευνα, που μπορεί να οδηγήσει σε ιδιαίτερος επιβαρυντικά για τους ίδιους στοιχεία.

II. Έννοια και αρχές της επεξεργασίας προσωπικών δεδομένων εργαζομένων

Ως δεδομένο προσωπικού χαρακτήρα λογίζεται, στο πλαίσιο του άρθρου 8 του Χάρτη, «κάθε πληροφορία σχετικά με φυσικό πρόσωπο η ταυτότητα του οποίου είναι

²² Βλ. ενδεικτικά Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ΕΕργΔ. 2018, σελ. 641επ.

²³ Σε σημείο μάλιστα που στη γερμανική βιβλιογραφία πολλές φορές γίνεται λόγος για «ιδιωτικοποίηση της ποινικής δίωξης» (“Privatisierung der Strafverfolgung”). βλ. Sauer σε Wabnitz/Janovsky, Hdb. Wirtschafts- und SteuerstrafR, Κεφ. 30 πλαγ.70επ.· Benz/Klindt, BB 2010, σελ.2979· Knauer, ZWH 2012, σελ.41· Taschke, NZWiSt 2012, σελ. 89· Brunhöber, GA 2010, σελ. 570· Greeve, StraFo 2013, σελ. 89· Knauer/Gaul, NStZ 2013, σελ. 192· Mansdörfer, JM 2014, σελ. 167· Schober, Focus Spezial 10-11/2017, σελ. 2, για «εξωτερική ανάθεση της ποινικής δίωξης» (“Outsourcing“ der Strafverfolgung”). Βλ. Brexl, AnwBl 2010, σελ. 498; πρβλ. Pfordte σε AG StrafR-DAV, Strafverteidigung im Rechtsstaat, σελ. 740, για «εξωτερική ανάθεση ερευνητικών δραστηριοτήτων» (“Auslagerung von Ermittlungshandlungen”). βλ. Pfordte σε AG StrafR-DAV, Strafverteidigung im Rechtsstaat, σελ. 740 ή για «πρόσληψη ιδιωτών για κρατικές ή ποινικές έρευνες» (“Indienstnahme Privater für hoheitliche bzw. strafrechtliche Ermittlungen“). βλ. Mansdörfer, JM 2014, σελ. 168.

γνωστή ή μπορεί να εξακριβωθεί»²⁴. Με πανομοιότυπο τρόπο προσεγγίζει την έννοια των προσωπικών δεδομένων ο Γ.Κ.Π.Δ. ορίζοντας στο άρθρο 4 ως προσωπικά δεδομένα όλες τις πληροφορίες που αναφέρονται σ' ένα φυσικό πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί εξακριβωθεί. Σε σχέση με την Οδηγία 95/46 ο Γ.Κ.Π.Δ. προσθέτει στον ορισμό των προσωπικών δεδομένων τα δεδομένα θέσης και επιγραμματικά αναγνωριστικά ταυτότητας, καθώς και τα γενετικά δεδομένα και βιομετρικά δεδομένα. Τα δεδομένα προσωπικού χαρακτήρα μπορεί να έχουν οποιαδήποτε μορφή, καθαρώς υλική²⁵ ή ηλεκτρονική²⁶. Έτσι στα δεδομένα προσωπικού χαρακτήρα εντάσσονται, μεταξύ άλλων, η διεύθυνση «IP» ενός υπολογιστή, η γεωγραφική θέση, ο τηλεφωνικός αριθμός και τα λοιπά στοιχεία επικοινωνίας ενός ατόμου²⁷ καθώς και το περιεχόμενο και τα δεδομένα κινήσεως οποιασδήποτε τηλεφωνικής ή διαδικτυακής του επικοινωνίας²⁸.

Το άρθρο 8 παρ.2εδ.α' του ΧΘΔΕΕ αναφέρεται στην «επεξεργασία» των δεδομένων προσωπικού χαρακτήρα. Το ΔΕΕ δεν έχει χρειαστεί να ορίσει το ίδιο την έννοια της «επεξεργασίας», καθώς αρχικά εφάρμοξε τον ορισμό που εμπεριείχετο στην καταργηθείσα Οδηγία 95/4640, ενώ πλέον εφαρμόζει τον μη ουσιωδώς διαφοροποιημένο ορισμό που περιλαμβάνει ο Γ.Κ.Π.Δ.. Βάσει του άρθρου 4παρ.2 του ενλόγω Κανονισμού, ως «επεξεργασία» προσωπικών δεδομένων ορίζεται «κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολο δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή». Η χρήση της λέξης «όπως» πριν από τις πράξεις που νοούνται ως επεξεργασία δεδομένων προσωπικού χαρακτήρα, υποδηλώνει τον ενδεικτικό χαρακτήρα της απαρίθμησης. Κατά τη νομολογία του ΔΕΕ,

²⁴ ΔΕΕ 24.11.2011, συνεκδικ. υποθ. C-468/10 και C-469/10, ASNEF, EU:C:2011:777, σκ.41-42· ΔΕΕ 3.10.2019, C-70/18, Α κ.ά., EU:C:2019:823, σκ.53-54.

²⁵ Βλ. ενδεικτικά ΔΕΕ 21.7.2011, C-104/10, Kelly, EU:C:2011:506, σκ. 22 και 54-56.

²⁶ Βλ. ενδεικτικά ΔΕΕ 14.2.2019, C-345/17, Sergejs Buivids, EU:C:2019:122, σκ.31-32.

²⁷ ΔΕΕ 8.4.2014, συνεκδικ. υποθ. C-293/12, Digital Rights Ireland, και C-594/12, Seitlinger κ.ά., EU:C:2014:238, σκ.16, 34 και 36· ΔΕΕ 26.7.2017, γνωμοδότηση 1/15 (συμφωνία PNR ΕΕ-Καναδά), EU:C:2016:656, σκ.30 και 93.

²⁸ Digital Rights Ireland, ανωτ. υποσημ. 27, σκ. 39-40 και 53-60. Βλ. και ΓΔ 11.6.2019, T-462/17, ΤΟ κ. Ευρωπαϊκού Οργανισμού Περιβάλλοντος (European Environmental Agency - EEA), EU:T:2019:397, σκ.193-203 και 244.

στην έννοια της επεξεργασίας εμπίπτουν επίσης η διατήρηση²⁹, η γνωστοποίηση³⁰, η παροχή πρόσβασης³¹ και η δημοσιοποίηση, συμπεριλαμβανομένης της αναρτήσεως στο διαδίκτυο³².

Ειδικά δε στις εργασιακές σχέσεις ως επεξεργασία προσωπικών δεδομένων νοείται κατ' αρχήν η επεξεργασία στο πλαίσιο σχέσης εξαρτημένης εργασίας, στην οποία προβαίνει ο εργοδότης ως «υπεύθυνος επεξεργασίας» ήδη από το προσυμβατικό στάδιο της διαδικασίας πρόσληψης του εργαζομένου κι έχει ως αντικείμενο τα προσωπικά δεδομένα του τελευταίου ως «υποκειμένου των δεδομένων»³³. Στην ίδια έννοια εμπίπτει και η επεξεργασία, η οποία γίνεται στο πλαίσιο δημοσιοϋπαλληλικής σχέσης με το Δημόσιο ή με το νομικό πρόσωπο δημοσίου δικαίου, όπου υπηρετεί ο δημόσιος υπάλληλος. Εν προκειμένω υποβάλλονται σε επεξεργασία προσωπικά δεδομένα του εν λόγω υπαλλήλου από το στάδιο της διαδικασίας επιλογής και διορισμού του μέχρι και το στάδιο που ακολουθεί την οριστική παύση της δημοσιοϋπαλληλικής σχέσης. Η ευρεία αυτή εννοιολογική προσέγγιση οφείλεται σε δύο λόγους: Πρώτον, επειδή η δημοσιοϋπαλληλική σχέση είναι ειδική κυριαρχική σχέση³⁴, στο πλαίσιο της οποίας ο δημόσιος υπάλληλος παρέχει την εργασία του υπό το καθεστώς μιας ιδιότυπης εξάρτησης από το Δημόσιο ή το νομικό πρόσωπο δημοσίου δικαίου και κατά τούτο εμφανίζει, τηρουμένων των αναλογιών, ομοιότητες με την σχέση εξαρτημένης εργασίας. Δεύτερον, επειδή οι κίνδυνοι που απειλούν την προσωπικότητα, την αξιοπρέπεια, τα θεμελιώδη δικαιώματα και τις ελευθερίες των δημοσίων υπαλλήλων, κατά την επεξεργασία αυτή, είναι οι ίδιοι με αυτούς που απειλούν τους εργαζόμενους με σχέση εξαρτημένης εργασίας. Σε αμφότερες τις ως άνω περιπτώσεις παρέχεται η ίδια προστασία από τον Γ.Κ.Π.Δ., στο μέτρο που επιτρέπουν οι ιδιαιτερότητες της εκάστοτε εργασιακής σχέσης³⁵. Προς επιβεβαίωση των ανωτέρω

²⁹ ΔΕΕ 21.12.2016, συνεκδικ. υποθ. C-203/15, Tele2 Sverige και C-698/15, Watson κ.ά., EU:C:2016:970, σκ.75· Digital Rights Ireland, ανωτ. υποσημ.27, σκ. 29.

³⁰ ΔΕΕ 21.7.2011, C-104/10, Kelly, EU:C:2011:506, σκ. 55-56.

³¹ ΔΕΕ 2.10.2018, C-207/16, Ministerio Fiscal, EU:C:2018:788, σκ. 37.

³² ΔΕΕ 9.11.2010, συνεκδικ. υποθ. C-92/09, Volker und Markus Schaecke GbR, και C-93/09, Eifert, EU:C:2010:662, σκ.50· ΓΔ 3.12.2015, T-314/13, CN κατά Κοινοβουλίου, EU:T:2015:926, σκ.52.

³³ Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ΕΕργΔ. 2018, σελ. 643· Δούκα, Η προστασία των προσωπικών δεδομένων στην σχέση εργασίας, εκδ. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2011 σελ. 7επ· Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 979, 82.

³⁴ Βλ. αντί πολλών Δημητρόπουλο, Συνταγματικά Δικαιώματα, εκδ. Σάκκουλα Αθήνα – Θεσσαλονίκη, β' εκδ. 2008, σελ. 88.

³⁵ Βλ. Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ΕΕργΔ. 2018, σελ. 645.

ο Έλληνας νομοθέτης περιέλαβε σχετική ρύθμιση στο άρθρο 27παρ.8 Ν.4624/2019³⁶, αξιοποιώντας την τεθείσα στον Κανονισμό «ρήτρα ανοίγματος» του άρθρου 88.

Σύμφωνα με το άρθρο 6 παρ.1 του Κανονισμού, η επεξεργασία είναι νόμιμη, εάν και εφόσον ισχύει ένας από τους περιοριστικά απαριθμούμενους λόγους νόμιμης επεξεργασίας. Συγκεκριμένα η επεξεργασία είναι σύννομη, εφόσον: α) πραγματοποιείται με την συγκατάθεση του υποκειμένου των δεδομένων, β) εντάσσεται στο πλαίσιο της εκπλήρωσης μια συμβατική σχέσης, γ) είναι αναγκαία για την εκπλήρωση υποχρέωσης από το νόμο, δ) αποσκοπεί στην διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων, ε) εξυπηρετεί την εκπλήρωση έργου δημοσίου συμφέροντος, στ) κρίνεται αναγκαία για την ικανοποίηση ενός έννομου συμφέροντος του υπεύθυνου επεξεργασίας, εφόσον δεν προέχει το συμφέρον του υποκειμένου των δεδομένων.

Όπως προκύπτει λοιπόν από το άρθρο 6 παρ.1 Γ.Κ.Π.Δ., ένας από τους νόμιμους λόγους επεξεργασίας προσωπικών δεδομένων είναι η συγκατάθεση του υποκειμένου των δεδομένων³⁷. Η πρόβλεψη αυτή τελεί σε πλήρη σύμπνοια με το άρθρο 8 παρ.2 εδ.α' Χ.Θ.Δ.Ε.Ε., σύμφωνα με το οποίο η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται *«για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου»*. Η συγκατάθεση διασφαλίζει την συμμετοχή του προσώπου στις αποφάσεις που αφορούν τη χρήση των δεδομένων του και αποτελεί εκδήλωση του δικαιώματος πληροφοριακής αυτοδιάθεσης του υποκειμένου των δεδομένων³⁸. Για να αναπτύσσει δε την νομιμοποιητική της λειτουργία, πρέπει να είναι: α) «ελεύθερη», να μην αποτελεί δηλαδή προϊόν εξαναγκασμού, καταναγκασμού, εκφοβισμού ή πλάνης, β) «συγκεκριμένη», να συνδέεται δηλαδή προς πράξη (ή προς σειρά πράξεων) επεξεργασίας με καθορισμένο σκοπό και γ) «εν πλήρει επιγνώσει» με την έννοια ότι ο ενδιαφερόμενος διαθέτει, κατά τον χρόνο παροχής της συγκαταθέσεώς του, ουσιώδεις πληροφορίες σχετικά με βασικές πτυχές της επεξεργασίας των

³⁶ Σύμφωνα με τη διάταξη αυτή *«Για τους σκοπούς του παρόντος νόμου ως εργαζόμενοι νοούνται οι απασχολούμενοι με οποιαδήποτε σχέση εργασίας ή σύμβαση έργου ή παροχής υπηρεσιών στο δημόσιο και στον ιδιωτικό φορέα, ανεξαρτήτως του κύρους της σύμβασης, οι υποψήφιοι για εργασία και οι πρώην απασχολούμενοι»*.

³⁷ Ως «συγκατάθεση» ορίζεται *«κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν»* (άρθρ. 4παρ.11 Κανονισμού). Βλ και άρθρο 3 παρ.15 κανονισμού 2018/1725.

³⁸ Δούκα, Η προστασία των προσωπικών δεδομένων στην σχέση εργασίας, εκδ. Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2011 σελ. 55· Ζερδελής, Εργατ.Δικ., εκδ. 2019, σελ. 979, 82.

δεδομένων του³⁹. Η απαίτηση για «ρητή» ένδειξη βουλήσεως αποκλείει κάθε πιθανότητα σιωπηρής συναγωγής της συγκατάθεσης, λόγου χάριν σε περιπτώσεις όπου ο ενδιαφερόμενος απλώς ενημερώθηκε για την επικείμενη επεξεργασία των δεδομένων του χωρίς να του ζητηθεί να την εγκρίνει⁴⁰.

Η συγκατάθεση του υποκειμένου των δεδομένων, ως ένας από τους λόγους που καθιστά νόμιμη την επεξεργασία και χρήση των προσωπικών δεδομένων, ειδικά στον χώρο των εργασιακών σχέσεων προκαλεί εύλογους προβληματισμούς, σε σημείο μάλιστα που να έχει αμφισβητηθεί ο παραπάνω νομιμοποιητικός χαρακτήρας της από μερίδα της θεωρίας⁴¹. Οι προβληματισμοί⁴² εντοπίζονται κυρίως στο γεγονός ότι η σχέση εργασίας αποτελεί χαρακτηριστικό παράδειγμα στο οποίο, λόγω της εξάρτησης του εργαζόμενου από τον εργοδότη, η συγκατάθεση του εργαζόμενου, ως υποκειμένου των δεδομένων, δεν αναμένεται να είναι ελεύθερη, επειδή είναι εμφανής ο φόβος, αν όχι ο πραγματικός κίνδυνος, να υποστεί ο εργαζόμενος δυσμενείς συνέπειες από την άρνηση χορήγησης ή την τροποποίηση ή την ανάκληση της συγκατάθεσης του⁴³. Ωστόσο θεσμικά στον Γ.Κ.Π.Δ. προκρίθηκε η άποψη, που ναι μεν δέχεται τον νομιμοποιητικό χαρακτήρα της συγκατάθεσης για την επεξεργασία προσωπικών δεδομένων του εργαζομένου, τον εξαρτά όμως από τον απαραίτητο όρο να είναι ελεύθερη η εν λόγω συγκατάθεση, ήτοι να παρέχεται από εργαζόμενο που δεν τελεί υπό καθεστώς φόβου ή κίνδυνου να υποστεί δυσμενείς συνέπειες από την άρνηση χορήγησης ή την τροποποίηση ή την ανάκληση της συγκατάθεσής του⁴⁴.

³⁹ CN, ανωτ. υποσημ.32, σκ.57-61.

⁴⁰ Volker, ανωτ. υποσημ. 32, σκ.63-64· CN, ανωτ. υποσημ.32, σκ.62 και 74-76.

⁴¹ Παπαϊωάννου, Ο έλεγχος από τον εργοδότη της ηλεκτρονικής αλληλογραφίας και της ενασχόλησης του μισθωτού με το διαδίκτυο, ΕΕργΔ 2006, σελ. 729· Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το γενικό κανονισμό προστασίας δεδομένων, σελ. 96· Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ΕΕργΔ. 2018, σελ. 653. Την θέση ότι η συγκατάθεση δεν αποτελεί νομιμοποιητικό λόγο για την επεξεργασία ούτε στις πλατφόρμες εργασίας υποστηρίζει η ομάδα Εργασίας του άρθρου 29 και στην Γνώμη 3/2017 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των συνεργατικών κυριών συστημάτων μεταφορών (6475) της 4η Οκτωβρίου 2017.

⁴² Παρόμοιους προβληματισμούς εκφράζει ο Ενωσιακός νομοθέτης και στην αιτ. σκ. 43 του ΓΚΠΔ, όπου ειδικότερα σημειώνεται ότι «η συγκατάθεση δεν θα πρέπει να παρέχει έγκυρη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μια συγκεκριμένη περίπτωση, όταν υπάρχει σαφής ανισότητα μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, ιδίως στις περιπτώσεις που ο υπεύθυνος επεξεργασίας είναι δημόσια αρχή και είναι επομένως σχεδόν απίθανο να έχει δοθεί η συγκατάθεση ελεύθερα σε όλες τις περιστάσεις αυτής της ειδικής κατάστασης».

⁴³ Βλ. Δούκα, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ΕΕργΔ. 2018, σελ. 652· Ζερδελέη, Εργατ. Δικ., εκδ. 2019, σελ. 978, 87.

⁴⁴ Βλ. την σκέψη 42 του προοιμίου του Κανονισμού.

Η άποψη αυτή διαπνέει και το άρθρο 27παρ.2 Ν.4624/2019, το οποίο παρέχει στον εφαρμοστή του δικαίου κατευθυντήριες γραμμές για την αξιολόγηση του οικειοθελούς χαρακτήρα της συγκατάθεσης ενός εργαζομένου⁴⁵. Σύμφωνα με τη διάταξη αυτή, για να κριθεί η συγκατάθεσή του ως αποτέλεσμα ελεύθερης επιλογής «πρέπει να λαμβάνονται υπόψη κυρίως: α) η υφιστάμενη στη σύμβαση εργασίας εξάρτηση του εργαζομένου και β) οι περιστάσεις κάτω από τις οποίες χορηγήθηκε η συγκατάθεση»⁴⁶. Για την αξιολόγηση, λοιπόν, του οικειοθελούς χαρακτήρα της συγκατάθεσης του εργαζομένου, λαμβάνεται υπόψη το σύνολο των περιστάσεων που συντρέχουν σε ορισμένη περίπτωση και συγκροτούν, in concreto, την εργασιακή σχέση⁴⁷. Όπως σημειώνεται στην Αιτιολογική Έκθεση του Ν. 4624/2019, η συγκατάθεση του εργαζομένου θεωρείται αποτέλεσμα ελεύθερης βούλησης, ιδίως στις περιπτώσεις, κατά τις οποίες η επεξεργασία των προσωπικών του δεδομένων συνδέεται με ένα νομικής ή οικονομικής φύσεως πλεονέκτημα που χορηγείται σ' αυτόν. Τούτο συμβαίνει για παράδειγμα, όταν παρέχεται η δυνατότητα στον εργαζόμενο να χρησιμοποιεί για ιδιωτική χρήση τα λειτουργικά συστήματα Η/Υ της επιχείρησης ή όταν τα συμφέροντα εργοδότη και εργαζομένου συγκλίνουν, όπως λ.χ. στη χρήση φωτογραφιών στο ενδοδίκτυο -intranet- με την έννοια ότι οι εργαζόμενοι και εργοδότες αλληλοεπιδρούν στο χώρο της επιχείρησης⁴⁸.

Ειδικά για την περίπτωση αυτοματοποιημένης επεξεργασίας με συγκατάθεση ή όταν αυτή είναι απαραίτητη για την εκτέλεση της σύμβασης, ο Γ.Κ.Π.Δ. στις γενικές ρυθμίσεις για την αυτοματοποιημένη επεξεργασία επαναλαμβάνει την ανάγκη εφαρμογής των γενικών αρχών διασφάλισης και λήψης των κατάλληλων μέτρων προστασίας (άρθρ. 22παρ.3). Γι' αυτό κατ' ελάχιστο πρέπει να είναι δυνατή η

⁴⁵ Σύμφωνα με την αιτιολογική σκέψη 155, βάσει της ρήτρας του άρθρου 88 παράγραφος 1 του ΓΚΠΔ, μπορούν να θεσπίζονται εσωτερικοί κανόνες ιδίως για τους όρους υπό τους οποίους δεδομένα προσωπικού χαρακτήρα στο πλαίσιο της απασχόλησης μπορούν να υφίστανται επεξεργασία με βάση τη συγκατάθεση του εργαζομένου.

⁴⁶ Πέραν των ανωτέρω κριτηρίων εξακολουθούν να ισχύουν και οι παράλληλες απαιτήσεις του ΓΚΠΔ, οι οποίες δεν σχετίζονται ειδικά με το πλαίσιο της απασχόλησης, όπως λ.χ το άρθρο 7παρ.4, σύμφωνα με το οποίο «Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαίτερα υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης».

⁴⁷ Κατά το μετρώ που γίνεται δεκτή η συγκατάθεση στις εργασιακές σχέσεις, ειδικά στις επιχειρήσεις με πολλούς εργαζόμενους, το γεγονός ότι η συγκατάθεση δόθηκε από την πλειοψηφία των εργαζομένων δεν νομιμοποιεί την επεξεργασία δεδομένων για όσους εργαζόμενους δε δίνουν τη συγκατάθεσή τους, γιατί η συγκατάθεση προϋποθέτει ατομική βούληση. ΣτΕ 94/2003, ΝΟΜΟΣ (περίπτωση συγκατάθεσης από 144 υπάλληλους τράπεζας, η οποία δε δεσμεύει εκείνους που δεν έδωσαν τη συγκατάθεσή τους).

⁴⁸ Παρόμοια είναι και τα κριτήρια που υιοθετήθηκαν στην αντίστοιχη διάταξη (άρθρ. 26 παρ.2) του νέου Ομοσπονδιακού Γερμανικού Νόμου για την προστασία των προσωπικών δεδομένων, που θεσμοθετήθηκε σε εκτέλεση της «ρήτρας ανοίγματος» του άρθρου 88παρ.1 ΓΚΠΔ.

παρέμβαση του εργαζομένου, καθώς η δυνατότητα αυτή συνεχεται άμεσα με τα δικαιώματα διαγραφής, περιορισμού της επεξεργασίας, φορητότητας, εναντίωσης και μη αυτοματοποιημένης λήψης απόφασης που προβλέπονται στα άρθρα 17-22 του ΓΚΠΔ. Η δοθείσα συγκατάθεση δεν πρέπει να δεσμεύει το υποκείμενο των δεδομένων εις το διηνεκές, καθώς τούτο θα συνεπαγόταν την πλήρη αποστέρηση του προσώπου αυτού από την προστασία του άρθρου 8 του Χάρτη, ιδίως σε περίπτωση μεταβολής των συνθηκών υπό τις οποίες παρείχε τη συγκατάθεσή του. Για να είναι σε θέση να ασκεί αποτελεσματικά το δικαίωμά του στην προστασία των δεδομένων του, ευλόγως προβλέφθηκε στο παράγωγο ενωσιακό δίκαιο ότι ο ενδιαφερόμενος έχει τη δυνατότητα να ανακαλεί, και μάλιστα ανά πάσα στιγμή, τη συγκατάθεσή του. Κατ' επέκταση, δικαιούται να εναντιώνεται σε επεξεργασία των δεδομένων του λαμβάνουσα χώρα έπειτα από την έγκυρη ανάκληση της συγκατάθεσής του που συνδεόταν με την επεξεργασία αυτή⁴⁹.

Πάντως και χωρίς τη συγκατάθεσή του εργαζόμενου, ο εργοδότης, ως υπεύθυνος επεξεργασίας, δικαιούται να προβεί σε επεξεργασία των προσωπικών δεδομένων των εργαζομένων, εφόσον η επεξεργασία μπορεί να βασιστεί σε κάποια από τις λοιπές περιπτώσεις των άρθρων 6 παρ.1 και 9 παρ.2 του Κανονισμού⁵⁰.

Η ύπαρξη ενός από τους νόμιμους λόγους επεξεργασίας των προσωπικών δεδομένων δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωση τήρησης των αρχών που πρέπει να διέπουν την επεξεργασία προσωπικών δεδομένων, όπως άλλωστε προβλέπεται ρητά και στο άρθρο 27παρ.5 του Ν.4624/2019. Πρόκειται για τις αρχές του σκοπού, της αναλογικότητας, της ακρίβειας, του χρονικού περιορισμού της περιόδου αποθήκευσης, της ασφάλειας και της λογοδοσίας (άρθρ. 5 Κανονισμού)⁵¹. Η επεξεργασία θα πρέπει να γίνεται για σκοπούς νόμιμους, σαφείς, συγκεκριμένους και προκαθορισμένους. Ο σκοπός είναι νόμιμος, όταν η επεξεργασία επιδιώκει την ικανοποίηση θεμιτών και αξίων προστασίας συμφερόντων του υπευθύνου επεξεργασίας. Συνεπώς νόμιμοι σκοποί για επεξεργασία στο πλαίσιο των εργασιακών σχέσεων είναι όσοι συνδέονται με τις ανάγκες κατάρτισης, λειτουργίας και λήξης της εργασιακής σχέσης. Όσον αφορά τα ευαίσθητα προσωπικά δεδομένα (στα οποία πλέον ο Κανονισμός αναφέρεται με τον όρο «ειδικές κατηγορίες

⁴⁹ Βλ. ΔΕΕ 24.9.2019, C-136/17, GC κ ά EU:C:2019:773, σκ.62.

⁵⁰ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 979, 88.

⁵¹ Οι αρχές αυτές, πλην αυτών της ασφάλειας και της λογοδοσίας, προβλέπονταν και στην Οδηγία 96/46.

δεδομένων»), θεωρείται η επεξεργασία τους απαγορευμένη και μόνο κατ' εξαίρεση επιτρέπεται, όταν συντρέχουν ειδικές περιστάσεις (άρθρ. 9 Γ.Κ.Π.Δ).

Ειδικότερα στο άρθρο 9 περ.2β' του Κανονισμού, που ενδιαφέρει τις εργασιακές σχέσεις, προβλέπεται ότι η επεξεργασία είναι δυνατή, όταν είναι απαραίτητη *«για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπεύθυνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους-μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων»*. Σύμφωνα με τη διάταξη αυτή, οι εθνικές ρυθμίσεις για να είναι συμβατές με τον Κανονισμό, θα πρέπει να προβλέπουν ότι η δυνατότητα επεξεργασίας θα συνοδεύεται από κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου, εν προκειμένω του εργαζόμενου, και κατά προέκταση να διασφαλίζονται οι γενικές αρχές που διέπουν την εν λόγω επεξεργασία⁵². Τέλος το άρθρο 88 παρ. 1 του Κανονισμού απαριθμεί ενδεικτικά ορισμένους νόμιμους σκοπούς για την επεξεργασία στο πλαίσιο των εργασιακών σχέσεων⁵³.

Κεντρική θέση μεταξύ των αρχών που διέπουν την επεξεργασία προσωπικών δεδομένων κατέχει η αρχή της αναλογικότητας, η οποία αποτελεί το κατ' εξοχήν κριτήριο ελέγχου της νομιμότητας της επεξεργασίας, όπως προκύπτει και από αποφάσεις της ΑΠΔΠΧ⁵⁴. Ο Κανονισμός απαιτεί τα προσωπικά δεδομένα να είναι *«κατάλληλα, συναφή και να περιορίζονται στα αναγκαία για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία»*, προσδιορίζοντας την ανωτέρω αρχή -κατά το εν προκειμένω λειτουργικό της νόημα- ως αρχή της ελαχιστοποίησης των δεδομένων.

⁵² Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το γενικό κανονισμό προστασίας δεδομένων, σελ. 103.

⁵³ Ειδικότερα σύμφωνα με την παράγραφο 1 του εν λόγω άρθρου, τα κράτη μέλη μπορούν να θεσπίζουν ειδικούς κανόνες για τη διασφάλιση της προστασίας των δικαιωμάτων και των ελευθεριών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης *«ιδίως για σκοπούς πρόσληψης, εκτέλεσης της σύμβασης απασχόλησης, συμπεριλαμβανομένης της εκτέλεσης των υποχρεώσεων που προβλέπονται από τον νόμο ή από συλλογικές συμβάσεις, διαχείρισης, προγραμματισμού και οργάνωσης εργασίας, ισότητας και πολυμορφίας στον χώρο εργασίας, υγείας και ασφάλειας στην εργασία, προστασίας της περιουσίας εργοδοτών και πελατών και για σκοπούς άσκησης και απόλαυσης, σε ατομική ή συλλογική βάση, δικαιωμάτων και παροχών που σχετίζονται με την απασχόληση και για σκοπούς καταγγελίας της σχέσης απασχόλησης»*.

⁵⁴ Βλ. ενδεικτικά τις υπ' αριθμόν 29/2-4-2018, 25/14-6-2021 και 39/3-9-2021 αποφάσεις της ΑΠΔΠΧ, όλες δημοσιευμένες στην ιστοσελίδα της Αρχής Προστασίας Δεδομένων ([url: https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=&field_year_to=&field_category=All&field_thematic=All&field_protocol_number=&field_keywords=αναλογικότητα](https://www.dpa.gr/el/enimerwtiko/prakseisArxis?field_year_from=&field_year_to=&field_category=All&field_thematic=All&field_protocol_number=&field_keywords=αναλογικότητα)).

Ειδικά δε στο πεδίο των εργασιακών σχέσεων, η συλλογή και επεξεργασία προσωπικών δεδομένων του εργαζόμενου επιτρέπεται, όπως γίνεται δεκτό⁵⁵, μόνον όταν αυτή υπηρετεί το σκοπό της σύμβασης εργασίας και περιορίζεται στα δεδομένα εκείνα που είναι αναγκαία ενόψει του ειδικότερου κάθε φορά σκοπού συλλογής και επεξεργασίας. Η άποψη αυτή αποτυπώνεται και στην πρώτη παράγραφο του άρθρου 27 Ν. 4624/2019, σύμφωνα με την οποία *«Δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να υποβάλλονται σε επεξεργασία για σκοπούς της σύμβασης εργασίας, εφόσον είναι απολύτως απαραίτητο για την απόφαση σύναψης σύμβασης εργασίας ή μετά τη σύναψη της σύμβασης εργασίας για την εκτέλεσή της»*. Περαιτέρω, η συλλογή και επεξεργασία πρέπει να γίνεται κατά τέτοιο τρόπο, ώστε να επεμβαίνει όσο το δυνατόν λιγότερο στην προσωπική ζωή του εργαζόμενου. Έτσι στην περίπτωση που μπορούν να χρησιμοποιηθούν ηπιότερα μέσα επίτευξης του σκοπού για τον οποίο συγκεντρώνονται πληροφορίες, πρέπει αυτά να προτιμώνται⁵⁶.

Όπως σημειώνεται στην Αιτιολογική Έκθεση του Ν. 4624/2019, ο εργοδότης ως υπεύθυνος επεξεργασίας πρέπει να λαμβάνει μέτρα, ώστε τα πρόσωπα που βρίσκονται υπό την εποπτεία του κι έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, να τα επεξεργάζονται μόνο με βάση τις οδηγίες του, εκτός κι αν είναι νομικά υποχρεωμένα να τα επεξεργάζονται χωρίς τις οδηγίες εργοδότη τους. Το πεδίο εφαρμογής των ανωτέρω ρυθμίσεων καταλαμβάνει αφενός όλα τα υπό επεξεργασία προσωπικά δεδομένα, ακόμα κι όταν αυτά δεν αποθηκεύονται ούτε προορίζονται να αποθηκευτούν σε ένα σύστημα αρχειοθέτησης (παράγραφος 6) κι αφετέρου όλους τους απασχολούμενους με οποιαδήποτε σχέση εργασίας ή σύμβαση έργου ή παροχής υπηρεσιών στο δημόσιο και στον ιδιωτικό φορέα, ανεξαρτήτως του κύρους της σύμβασης, καθώς και τους υποψηφίους για εργασία και τους πρώην απασχολούμενους (παράγραφος 8). Στα άρθρα 33, 34 και 35 θεσπίζονται τα δικαιώματα πρόσβασης, διαγραφής κι εναντίωσης του υποκειμένου των δεδομένων, ενώ στα άρθρα 38 και 39 προβλέπονται ποινικές και διοικητικές κυρώσεις για τους παραβάτες του Γενικού Κανονισμού για την Προστασία Δεδομένων και του Ν.4624/2019.

⁵⁵ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 978, 88.

⁵⁶ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 978, 88.

III. Έννοια και φυσιογνωμία των εσωτερικών ερευνών

Στην έννοια των εσωτερικών ερευνών εντάσσονται όλες εκείνες οι ενέργειες, οι οποίες διεξάγονται στο εσωτερικό μιας εταιρείας για την διαλεύκανση περιπτώσεων μη συμμόρφωσης με τους κανόνες, που πρέπει να τηρούνται από τους εργαζομένους. Στους κανόνες αυτούς συγκαταλέγονται παραβιάσεις του ποινικού κώδικα, παραβιάσεις εσωτερικών κατευθυντήριων γραμμών της εταιρείας, αλλά και οποιαδήποτε ανάρμοστη συμπεριφορά από εργαζομένους της εταιρείας. Οι εσωτερικές έρευνες έχουν κατασταλακτικό χαρακτήρα και διενεργούνται από την ίδια την εταιρεία με δική της πρωτοβουλία και όχι για λογαριασμό του κράτους⁵⁷, είτε με τη χρήση ίδιων πόρων της εταιρείας, είτε με την υποστήριξη εξωτερικών ερευνητών. Θεωρούνται νόμιμες, καθώς δεν υφίσταται (ποινική ή άλλη) διάταξη που να τις απαγορεύει, μπορούν δε να διεξάγονται ακόμα και ταυτόχρονα με εισαγγελικές έρευνες, χωρίς να τίθεται ζήτημα είτε προσβολής του κρατικού μονοπωλίου στην επιβολή του νόμου⁵⁸ είτε νόσφισης εξουσίας⁵⁹.

Μάλιστα υπάρχουν περιπτώσεις, όπου επιβάλλεται η διενέργειά τους, προκειμένου αφενός να αποφευχθούν φορολογικές⁶⁰ ή άλλου είδους οικονομικές⁶¹ κυρώσεις της εταιρείας και να διασωθεί η φήμη της⁶² που έχει πληγεί από εγκληματικές ή ανάρμοστες συμπεριφορές των εργαζομένων της και αφετέρου να ενημερωθούν τρίτοι (π.χ. πελάτες, προμηθευτές) σχετικά με παραβιάσεις ή εσφαλμένους χειρισμούς των εργαζομένων, από τους οποίους ζημιώθηκαν⁶³. Άλλωστε, εάν δεν διενεργηθούν τέτοιου είδους έρευνες για την εξακρίβωση ποινικών αδικημάτων ή άλλων παραβιάσεων από τις οποίες ζημιώθηκε η εταιρεία, ενδέχεται να γεννηθούν ποινικές ευθύνες στα πρόσωπα των διοικούντων ή άλλων ατόμων που ασκούν διαχειριστικά καθήκοντα. Ειδικότερα γίνεται δεκτό⁶⁴ ότι λόγω της υποχρέωσης πίστης που φέρουν

⁵⁷ Wilkens, Internal Investigations, σελ. 53, 82· Salvenmoser/Schreier σε Achenbach/Ransiek, Hdb. Wirtschaftsstrafrecht, σελ. 1673, πλαγ. 13· πρβλ. επίσης: Rotsch σε Rotsch, Criminal Compliance, § 2 B πλαγ. 24 („separat von der staatlichen Ermittlungstätigkeit“). Scharnberg, Illegale Internal Investigations, σελ. 27· Greeve, StraFo 2013, σελ. 89· Wisskirchen/Glaser, DB 2011, σελ. 1392.

⁵⁸ Wilkens, Internal Investigations, σελ. 79.

⁵⁹ BGH NJW 1994, 1228-1229· Fischer, StGB, §132 πλαγ. 3.

⁶⁰ Wilkens, Internal Investigations, σελ. 111.

⁶¹ Wilkens, Internal Investigations, σελ. 90επ.

⁶² Wilkens, Internal Investigations, σελ. 132επ.

⁶³ BGH GRUR 1987, 647· NJW 1986, 1247, 1249· 1978, 1002· OLG Düsseldorf Urt. v. 8.6.2006 - 2 U 28/05, juris· LAG Hamm CCZ 2010, 237, 238· LAG Rheinland-Pfalz BeckRS 2008, 51666· LAG Berlin NZA 1993, 27.

⁶⁴ Wilkens, Internal Investigations, σελ. 140· Kirsch σε Kempf/Lüderssen/Volk, Unternehmensstrafrecht, σελ. 362· v. Rosen, Internal Investigations, σελ. 66· Golombek, WiJ 2012, σελ.

τα μέλη της διοίκησης έναντι της εταιρείας, οφείλουν σε περιπτώσεις παράτυπων ή παράνομων ενεργειών των εργαζομένων να προβαίνουν σε όλες τις δέουσες ενέργειες για την αποτροπή της επανάληψής τους και παράλληλα να ασκούν εγκαίρως αξιώσεις αποζημίωσης, που γεννιούνται στο πρόσωπο της εταιρείας. Εάν δεν συμμορφωθούν με την υποχρέωσή τους αυτή, επέχουν ευθύνη για παραβίαση των κανόνων επιμελούς διαχείρισης των συμφερόντων της εταιρείας και μπορεί να στοιχειοθετηθεί στα πρόσωπά τους ποινική ευθύνη για απιστία (άρθρ. 390 ΠΚ) λόγω μη λήψης όλων των οφειλόμενων μέτρων για την διαφύλαξη της περιουσίας της⁶⁵. Επίσης λόγω της εγγυητικής θέσης που έχουν τα μέλη της διοίκησης ή ένα διευθυντικό στέλεχος έναντι της εταιρείας, γίνεται δεκτό⁶⁶ ότι σε περίπτωση που παραλείπουν να λάβουν διερευνητικά μέτρα για την εξιχνίαση κάποιας αξιόποινης συμπεριφοράς εργαζομένου, μπορούν να θεωρηθούν ως συμμέτοχοι σ' αυτή⁶⁷, εάν η παράλειψή τους διευκολύνει τη διάπραξη περαιτέρω αδικημάτων ή προωθεί με κάποιον τρόπο την ήδη τελούμενη εγκληματική δραστηριότητα.

Από τα ανωτέρω γίνεται αντιληπτό ότι ο εργοδότης όχι μόνο έχει δικαίωμα να προβαίνει σε εσωτερικές έρευνες για την εξιχνίαση εγκληματικών ή ανάρμοστων συμπεριφορών των εργαζομένων του, με απώτερο σκοπό να προστατέψει την εταιρεία του και τα προσωπικά συμφέροντά του, αλλά παράλληλα έχει καθήκον να αναλαμβάνει τέτοιου είδους πρωτοβουλίες, προκειμένου να μη βρεθεί ο ίδιος φορολογικά, ποινικά ή αστικά υπόλογος για πράξεις ή παραλείψεις των εργαζομένων του, από τις οποίες

165· Heutz, DB 2012, σελ. 902· Knauer, ZWH 2012, σελ. 47· Kuhlen, NZWist 2015, σελ. 126. Αναλυτικά σχετικά με την ποινική ευθύνη λόγω παραίτησης της εταιρείας από αξίωση αποζημίωσης κατά μελών εταιρικών οργάνων ή υπαλλήλων βλ. Hoffmann/Wißmann, StV 2001, σελ. 249επ· Kahlenberg/Schwinn, CCZ 2012, σελ. 85· Poller, StraFo 2005, σελ. 274επ· Schott, StraFo 2014, σελ. 315επ· Spatscheck/Ehnert, StraFo 2005, σελ. 265επ· Werner, CCZ 2011, σελ. 201επ.

⁶⁵ Wilkens, Internal Investigations, σελ. 140· Kirsch in Kempf/Lüderssen/Volk, Unternehmensstrafrecht, σελ. 362; v. Rosen, Internal Investigations, σελ. 66; Golombek, WiJ 2012, σελ. 165; Heutz, DB 2012, σελ. 902; Knauer, ZWH 2012, σελ. 47; Kuhlen, NZWist 2015, σελ. 126. Αναλυτικά σχετικά με την ποινική ευθύνη λόγω παραίτησης της εταιρείας από αξίωση αποζημίωσης κατά μελών εταιρικών οργάνων ή υπαλλήλων βλ. Hoffmann/Wißmann, StV 2001, σελ. 249επ· Kahlenberg/Schwinn, CCZ 2012, σελ. 85· Poller, StraFo 2005, σελ. 274επ· Schott, StraFo 2014, σελ. 315επ· Spatscheck/Ehnert, StraFo 2005, σελ. 265επ· Werner, CCZ 2011, σελ. 201επ.

⁶⁶ Wilkens, Internal Investigations, σελ. 150, όπου και περαιτέρω παραπομπές.

⁶⁷ Ωστόσο στην περίπτωση αυτή για την στοιχειοθέτηση ποινικής ευθύνης απαιτείται να αποδεικνύεται αφενός η αιτιότητα ανάμεσα στην παράλειψη λήψης διερευνητικών μέτρων από την διοίκηση της εταιρείας ή τα διευθυντικά στελέχη της και στη συνεχιζόμενη διάπραξη εγκληματικών συμπεριφορών και αφετέρου ο δόλος (έστω και ενδεχόμενος) του δράστη, που έγκειται στο ότι γνωρίζει την συνεχιζόμενη η επικείμενη τέλεση μιας αξιόποινης πράξης και τουλάχιστον την αποδέχεται. Με άλλα λόγια ο διοικητής ή διαχειριστής της εταιρείας θα πρέπει τουλάχιστον να έχει μια εύλογα συγκεκριμένη αντίληψη ως προς τις εγκληματικές συμπεριφορές τη διάπραξη των οποίων διευκολύνει μέσω της παράλειψής του. Βλ. Wilkens, Internal Investigations, σελ. 153· Wessing/Dann σε Bürkle/Hauschka, Der Compliance Officer, § 9 πλαγ. 102· Wybitul, BB 2009, σελ. 2591.

έχουν προκληθεί ζημιές στην εταιρεία, στο κράτος ή και σε τρίτους (λ.χ. πελάτες, προμηθευτές). Για να αποφευχθούν, ωστόσο, καταχρηστικές συμπεριφορές εκ μέρους του εργοδότη, οι οποίες μπορούν να θέσουν σε κίνδυνο συνταγματικά αγαθά και δικαιώματα των εργαζομένων, τίθεται ως προϋπόθεση για την ανάληψη μιας τέτοιας πρωτοβουλίας να υφίσταται ένας συγκεκριμένος βαθμός υποψίας σε βάρος του εργαζομένου.

Κατ' αρχάς γίνεται δεκτό⁶⁸ ότι απλές φήμες και αόριστοι ισχυρισμοί (π.χ. ο εργαζόμενος Α είναι αναξιόπιστος) δεν αρκούν για να νομιμοποιήσουν τη διενέργεια μιας εσωτερικής έρευνας, εκτός κι αν πρόκειται για πράξη που τελείται σε συστηματική βάση, με αποτέλεσμα να παράγονται σοβαρές οικονομικές συνέπειες για την εταιρεία⁶⁹. Στη γερμανική θεωρία, προκειμένου να καθοριστεί ο απαιτούμενος βαθμός υποψίας, προτείνεται ο προσανατολισμός σ' εκείνες τις διατάξεις του Κώδικα Ποινικής Δικονομίας, βάσει των οποίων αρκούν απλές ενδείξεις βασισμένες σε συγκεκριμένα γεγονότα και δεν απαιτούνται πλήρη αποδεικτικά στοιχεία⁷⁰. Ωστόσο, μία τέτοια προσκόλληση στις αρχές που θεσπίζει ο Κώδικας Ποινικής Δικονομίας, δεν κρίνεται σκόπιμη, αν αναλογιστούμε ότι, σε αντίθεση με τις εισαγγελικές αρχές, τα μέλη του διοικητικού συμβουλίου μιας εταιρείας δεν έχουν ως κύριο μέλημα τη διερεύνηση παραβιάσεων του νόμου, αλλά τη διαχείριση της περιουσίας και εν γένει των συμφερόντων της. Άλλωστε, οι υποχρεώσεις έρευνας στο πλαίσιο του εταιρικού δικαίου διαφέρουν σημαντικά και είναι δύσκολο να συγκριθούν με εκείνες του ποινικού δικονομικού δικαίου από την σκοπιά της αιτίας και του σκοπού⁷¹. Ως εκ τούτου, μια αξιολόγηση του βαθμού της υποψίας βασιζόμενη, κατά περίπτωση, στην

⁶⁸ Wilkens, Internal Investigations, σελ. 200· Grützner in Momsen/Grützner, Wirtschaftsstrafrecht, Κεφ. 4 πλαγ. 52· Reichert, ZIS 2011, σελ.117· Wisskirchen/Glaser, DB 2011, σελ.1394· πρβλ.: Hüffer/Koch, AktG, § 111 πλαγ. 8· αλλά επίσης Theile/Gatter/Wiesenack, ZStW 2014, σελ. 823.

⁶⁹ Fuhrmann, NZG 2016, σελ. 885· Ott/Lüneborg, CCZ 2019, σελ. 76· Grützner in Momsen/Grützner, Wirtschaftsstrafrecht, κεφ. 4 πλαγ. 54.

⁷⁰ Grützner in Momsen/Grützner, Wirtschaftsstrafrecht, Κεφ. 4 πλαγ. 52· Bachmann, ZHR 2016, σελ. 571· Ott/Lüneborg, CCZ 2019, σελ. 76· βλ. επίσης: Fleischer in Fleischer, Hdb. d. Vorstandsrechts, § 8 πλαγ. 35. Βλ. και BGH NStZ 1994, 499.

⁷¹ Wilkens, Internal Investigations, σελ. 153· Grützner σε Momsen/Grützner, Wirtschaftsstrafrecht, Κεφ. 4 πλαγ. 52.

αξιοπιστία⁷² και τη βασιμότητα⁷³ των πληροφοριών καθώς και στη σοβαρότητα του διερευνώμενου παραπτώματος, κρίνεται πιο εύλογη⁷⁴.

Όπως είναι ευνόητο, οι εσωτερικές έρευνες του εργοδότη, λόγω του ιδιαίτερου επεμβατικού χαρακτήρα τους στα δικαιώματα των εργαζομένων, πρέπει να διενεργούνται με απόλυτο σεβασμό προς την προσωπικότητά τους και τις θεμελιώδεις συνταγματικές ελευθερίες τους. Πρωτίστως πρέπει να διαφυλάττονται τα προσωπικά δεδομένα τους, στο μέτρο που αυτά δε συνέχονται με το αντικείμενο της έρευνας και να ελαχιστοποιούνται οι πληροφορίες που συλλέγονται και ανάγονται στο θεμελιώδες δικαίωμα του πληροφοριακού αυτοπροσδιορισμού του. Ως νομιμοποιητικός λόγος αυτών των ερευνών προβάλλει η ικανοποίηση των εύλογων συμφερόντων του εργοδότη, ως υπεύθυνου επεξεργασίας, τα οποία, υπό τους όρους που αναφέρθηκαν παραπάνω, υπερισχύουν των συμφερόντων του εργαζομένου ως υποκειμένου των δεδομένων σύμφωνα με το άρθρο 6 παρ.1 περ.ε' Γ.Κ.Π.Δ.. Κατά τη διενέργεια των ερευνών πρέπει να τηρούνται οι αρχές επεξεργασίας των προσωπικών δεδομένων, όπως αυτές αποτυπώνονται στον Γ.Κ.Π.Δ. και στην εσωτερική νομοθεσία. Πρωτίστως δε οι πληροφορίες που συλλέγονται, δεν θα πρέπει να είναι δυσανάλογες ή άσχετες με τον επιδιωκόμενο σκοπό, βάσει της αρχής της αναλογικότητας, όπως αυτή κατοχυρώνεται στο άρθρο 6 παρ.1 περ.γ Γ.Κ.Π.Δ. και -σε επίπεδο πρωτογενούς ενωσιακού δικαίου- στο άρθρο 51 παρ. 1 του ΧΘΔΕΕ.

Κατόπιν των ανωτέρω, προσεγγίζεται στο επόμενο κεφάλαιο η συνηθέστερη μορφή επεξεργασίας δεδομένων, η οποία, στην σύγχρονη εποχή της τεχνολογικής προόδου επιστρατεύεται στο πλαίσιο των εσωτερικών ερευνών, με σκοπό την εξακρίβωση της διάπραξης τυχόν αξιόποινων ή άλλων παράτυπων πράξεων από τους

⁷² Πρβλ. και την κατάταξη στην οποία προβαίνει ο Fuhrmann (NZG 2016, σελ. 885) και σύμφωνα με την οποία ως πιο αξιόπιστες πηγές θεωρούνται οι επίσημες αρχές, οι εξωτερικοί σύμβουλοι της εταιρείας, κυρίως ο ελεγκτής [ή] ο μακροχρόνιος δικηγόρος που εμπιστεύεται η εταιρεία και επίσης δελτία τύπου από έγκριτες πηγές δημοσίευσης (*die „wohl authentischste Quelle dafür, dass im Unternehmen ‚etwas faul ist‘ [...] die Einleitung oder Ankündigung behördlicher Ermittlungen“ sei. Ähnlich ernst zu nehmende Hinweisgeber seien „die externen Hausberater des Unternehmens, allen voran der Abschlussprüfer [oder] der langjährige Anwalt des Vertrauens der Gesellschaft“ und „durchaus επίσης Presseveröffentlichungen seriöser Publikationsorgane“, während „sonstige Hinweise, namentlich von anonym bleibenden Arbeitnehmern oder Kunden [...] tendenziell eher mit Vorsicht zu genießen“ seien).*

⁷³ Κριτήρια θα μπορούσαν να αποτελέσουν η συχνότητα και η συνέπεια των πληροφοριών, δηλαδή εάν προέρχονται από διαφορετικές πηγές, αλλά παρ' όλα αυτά συμφωνούν σε μεγάλο βαθμό. Βλ. Fuhrmann, NZG 2016, σελ. 885 .

⁷⁴ Wilkens, Internal Investigations, σελ. 202· Grütznert σε Momsen/Grütznert, Wirtschaftsstrafrecht, Κεφ. 4 π.λαγ. 51 επ.· Poppe in Inderst/Bannenberg/Poppe, Compliance, Κεφ. 6 π.λαγ. 23· Fuhrmann, NZG 2016, σελ. 885· Hugger, ZHR 2015, σελ. 216, 219 επ.· Wagner, CCZ 2009, σελ. 12· πρβλ. επίσης: Hölters σε Hölters, AktG, § 93 π.λαγ. 168; Rönnau/Schneider, ZIP 2010, σελ. 59.

εργαζόμενους. Πρόκειται για την επεξεργασία των δεδομένων που διακινούνται μέσω ηλεκτρονικής αλληλογραφίας ή «φορτώνονται» από το διαδίκτυο και από τα οποία ο εργοδότης συγκεντρώνει πολλές φορές χρήσιμες πληροφορίες για παραβατικές συμπεριφορές των εργαζομένων. Παράλληλα, επιχειρείται να αναδειχθούν οι ποινικές ευθύνες που ενδέχεται να γεννηθούν στο πρόσωπο του εργοδότη από την μη τήρηση των υποχρεώσεών του ως υπευθύνου επεξεργασίας.

Κεφάλαιο τρίτο

Ζητήματα προστασίας θεμελιωδών δικαιωμάτων των εργαζομένων και ποινικής ευθύνης

Ι. Εισαγωγικές παρατηρήσεις

Στο σύγχρονο εργασιακό χώρο, όπου κυριαρχούν οι ηλεκτρονικοί υπολογιστές και τα διαδικτυακά δεδομένα, είναι φυσικό οι εσωτερικές έρευνες που διενεργούν οι εταιρείες, να εστιάζουν κυρίως σ' αυτά⁷⁵. Μεγάλες πολυεθνικές εταιρείες, οι οποίες διατηρούν γραφεία και θυγατρικές εταιρείες σε διάφορα μέρη του πλανήτη, βασίζονται, τις τελευταίες δεκαετίες, τη λειτουργία τους σε πολύπλοκα υπολογιστικά συστήματα, τα οποία συνεχώς εξελίσσονται, δίνοντας έτσι τη δυνατότητα στους εργαζομένους να διασυνδέονται και να ανταλλάσσουν πληροφορίες σχετικά με το εργασιακό τους αντικείμενο. Παράλληλα μεγάλες επιχειρήσεις ή όμιλοι επιχειρήσεων που λειτουργούν είτε σε διεθνές είτε σε εθνικό επίπεδο, επιλέγουν την ηλεκτρονική διασύνδεση των διαφόρων υποκαταστημάτων τους μέσω δικτύων υπολογιστών, τα οποία τους εξασφαλίζουν ταχύ, εύκολο και ασφαλή διαμοιρασμό δεδομένων και πληροφοριών μεταξύ των εργαζομένων τους και των πελάτων - προμηθευτών τους. Με την ανάπτυξη δε της τεχνολογίας και την επικράτηση της διαδικτυακής σύνδεσης σε όλους τους τομείς της οικονομίας, όλο και περισσότερες μικρομεσαίες επιχειρήσεις επιλέγουν να εξοπλίζουν τις εγκαταστάσεις τους με ηλεκτρονικούς υπολογιστές, μέσω των οποίων οι εργαζόμενοί τους μπορούν να επικοινωνούν είτε με προμηθευτές, προβαίνοντας σε παραγγελίες-οικονομικές διευθετήσεις είτε με πελάτες και το ευρύτερο αγοραστικό κοινό, πωλώντας τους προϊόντα και διαφημίζοντάς τις προσφερόμενες υπηρεσίες. Παράλληλα, υπάρχουν και κατηγορίες εργαζομένων, που συνάπτουν διαδικτυακά συμβάσεις εξαρτημένης εργασίας με εταιρείες που δραστηριοποιούνται καθαρά στο εξωτερικό και που μέσα από κατάλληλες ηλεκτρονικές φόρμες προσφέρουν εργασία σε διάφορους υποψηφίους σε όλο τον κόσμο, οι οποίοι το μόνο που έχουν να κάνουν είναι να αποδεχθούν τους προτεινόμενους όρους εργασίας συμπληρώνοντας τα στοιχεία τους σε προδιατυπωμένες ηλεκτρονικές φόρμες.

⁷⁵ Στη Γερμανία μία στις τρεις επιχειρήσεις βασίζεται κατά βάση στην ανάλυση του ηλεκτρονικού ταχυδρομείου των εργαζομένων, προκειμένου να αντλήσει στοιχεία στο πλαίσιο εσωτερικών ερευνών. Βλ. KPMG, Wirtschaftskriminalität 2018, σελ. 29. Μέχρι σήμερα δεν έχουν συλλεχθεί αντίστοιχα στατιστικά δεδομένα για τις ελληνικές επιχειρήσεις.

Σ' όλες τις παραπάνω περιπτώσεις οι εργοδότες παρέχουν στους εργαζομένους τους πρόσβαση στα ηλεκτρονικά συστήματα της επιχείρησης, προκειμένου να εκτελούν ευκολότερα και γρηγορότερα τα εργασιακά καθήκοντά τους και να προωθούν αποτελεσματικότερα τα συμφέροντα της επιχείρησης. Αναλόγως δε με την πολιτική του εργοδότη, άλλοτε παρέχεται στους εργαζόμενους ακώλυτη πρόσβαση στο διαδίκτυο και στην ηλεκτρονική αλληλογραφία τους κι άλλοτε περιορίζεται η πρόσβαση αυτή σε συγκεκριμένες ιστοσελίδες και σε συγκεκριμένο υπηρεσιακό ηλεκτρονικό ταχυδρομείο.

II. Η προστασία της ιδιωτικής ζωής του εργαζομένου

Ασχέτως πάντως της πολιτικής που ακολουθεί ο εκάστοτε εργοδότης, αναγνωρίζεται στο εργαζόμενο, ο οποίος καταναλώνει μεγάλο μέρος της καθημερινότητάς του στον εργασιακό χώρο, το δικαίωμα να αναπτύσσει μέρος της ιδιωτικής του ζωής κατά τη διάρκεια της εργασίας του⁷⁶. Έτσι μέρος της περιήγησής του στο διαδίκτυο που του εξασφαλίζει ο εργοδότης του, μπορεί να είναι αφιερωμένο σε εκφάνσεις της ιδιωτικής του ζωής, όπως π.χ. ταξίδια, αγορές, ψυχαγωγία, άθληση. Επίσης σε ένα μικρό συνήθως τμήμα του χρόνου εργασίας του μπορεί να επισκέπτεται τους προσωπικούς του λογαριασμούς ηλεκτρονικού ταχυδρομείου ή κοινωνικής δικτύωσης και να επικοινωνεί με γνώριμα του πρόσωπα, αποστέλλοντας μηνύματα και προβαίνοντας σε αναρτήσεις όχι μόνο από την επαγγελματική αλλά και από την ιδιωτική του ζωή. Άλλωστε είναι γεγονός ότι ορισμένες σύγχρονες εργασιακές πρακτικές που υιοθετούνται από επιχειρήσεις, με σκοπό την εξοικονόμηση οικονομικών πόρων και την καλύτερη οργάνωση και εκτέλεση των προσφερόμενων υπηρεσιών τους (όπως οι επιχειρησιακές πρακτικές «Bring your own Device»⁷⁷ και «Crowdwork»), συμπλέκονται άμεσα με την ιδιωτική ζωή των απασχολουμένων και καθιστούν δυσδιάκριτα τα όρια μεταξύ του ιδιωτικού και του επαγγελματικού τους

⁷⁶ ΕΔΔΑ αποφ. 16.12.1992 Niemietz κατά Γερμανίας

⁷⁷ Όταν ακολουθείται η επιχειρησιακή αυτή πρακτική, είναι σκόπιμο να διαχωρίζονται τα υπηρεσιακά από τα προσωπικά δεδομένα, για να μην υπάρχει κίνδυνος να αναμειχθούν ή να αποκτήσει ο εργοδότης πρόσβαση στα προσωπικά δεδομένα του εργαζομένου. Αυτό θα μπορούσε να εξασφαλισθεί είτε μέσω της παραχώρησης ειδικής κάρτας - SIM είτε μέσω της εγκατάστασης κάποιας εφαρμογής, όπως πχ. Sandbox - Apps ή Container - Apps. Σε κάθε περίπτωση πρέπει να προβλέπονται συγκεκριμένα διαχειριστικά μέτρα, προς αποτροπή πρόσβασης του εργοδότη στα προσωπικά δεδομένα των εργαζομένων που βρίσκονται αποθηκευμένα στις ιδιωτικές συσκευές του. Βλ. Baumgartner, Telefon-, Internet- und E-mail-Nutzung, einschließlich Privatnutzung (mit Betriebsvereinbarungsvorschlag im Praxishandbuch zum Arbeitnehmerdatenschutz, σελ. 368.

βίου. Τα όρια αυτά καθίστανται ακόμα πιο δυσδιάκριτα, αν αναλογιστεί κανείς ότι ορισμένες ενέργειες των εργαζομένων προσιδιάζουν τόσο σε υπηρεσιακούς όσο και σε ιδιωτικούς σκοπούς, όπως π.χ. η επίσκεψη ενός εργαζομένου σε ιστοσελίδα μετεωρολογικού σταθμού που γίνεται ενόψει ενός προγραμματισμένου επαγγελματικού ταξιδιού⁷⁸. Γίνεται δε δεκτό ότι σε περίπτωση αμφιβολίας θα πρέπει να δίνεται προτεραιότητα στον υπηρεσιακό χαρακτήρα μίας τέτοιας ενέργειας, ενόψει και των ευρύτερων συνθηκών εμφάνισής της⁷⁹.

Από τα παραπάνω γίνεται κατανοητό ότι η ιδιωτικότητα δεν περιορίζεται σε δράσεις στον ιδιωτικό χώρο ούτε σε ένα στενό κύκλο προσωπικών διαθέσεων, αλλά εκτείνεται σε δράσεις στον δημόσιο και στον εργασιακό χώρο. Το ΔΕΕ στην υπόθεση ΤΟ κ. ΕΟΠ⁸⁰ αναγνώρισε με πανηγυρικό τρόπο την ανάγκη προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων ενός ατόμου στο χώρο της εργασίας, στο μέτρο που λαμβάνει χώρα διακίνηση προσωπικής του αλληλογραφίας μη αφορώσας την εργασιακή σχέση του. Στη συγκεκριμένη υπόθεση υπάλληλοι του Ευρωπαϊκού Οργανισμού Περιβάλλοντος διακίνησαν μεταξύ τους μήνυμα ηλεκτρονικού ταχυδρομείου μιας άλλης υπαλλήλου, που αφορούσε διαπραγματεύσεις με κτηματομεσιτικό γραφείο για το διαμέρισμα όπου διέμενε και στο οποίο υπήρχαν διάφορα προσωπικά δεδομένα της, όπως το όνομά της, η διεύθυνση κατοικίας της και αποσπάσματα από μηνύματα ηλεκτρονικού ταχυδρομείου που είχαν συνταχθεί από την προσωπική της διεύθυνση ηλεκτρονικού ταχυδρομείου προς τον ιδιοκτήτη του διαμερισμάτος της. Σκοπός δε της διακίνησης ήταν η σύνταξη έκθεσης, η οποία, μετά από τρεις εβδομάδες, κοινοποιήθηκε στην υπάλληλο που αφορούσε, προκειμένου να ενημερωθεί για την επικείμενη απόλυσή της. Μετά την απόλυσή της η υπάλληλος προσέφυγε στο Πρωτοδικείο ζητώντας, μεταξύ άλλων, να επιδικαστεί στο πρόσωπό της αποζημίωση λόγω της ηθικής βλάβης που υπέστη από τη δημοσιοποίηση προσωπικών δεδομένων της. Το Δικαστήριο έκρινε ότι στην προκειμένη περίπτωση συνέτρεχε παραβίαση του άρθρου 8 του ΧΘΔΕΕ και ότι υπήρξε παράνομη πρόσβαση και χρήση προσωπικών δεδομένων της προσφεύγουσας, καθόσον ο μη επαγγελματικός

⁷⁸ Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το γενικό κανονισμό προστασίας δεδομένων, σελ. 112 -115.

⁷⁹ Baumgartner: Telefon-, Internet- und E-mail-Nutzung, einschließlich Privatnutzung (mit Betriebsvereinbarungsvorschlag) in: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis - Praxishandbuch zum Arbeitnehmerdatenschutz, hrsg. von Stephan Weth, Maximilian Herberger und Michael Wächter, 2014, σελ. 368.

⁸⁰ ΓΔ 11.6.2019, T-462/17, ΤΟ κ. Ευρωπαϊκού Οργανισμού Περιβάλλοντος (European Environmental Agency - EEA), EU:T:2019:397, σκ. 201-203.

χαρακτήρας της επίμαχης ηλεκτρονικής αλληλογραφίας δεν μπορούσε να αμφισβητηθεί· για τους λόγους αυτούς κάνοντας δεκτή την αίτησή της επιδίκασε στο πρόσωπό της την αποζημίωση λόγω ηθικής βλάβης.

Από την άλλη μεριά δεν αμφισβητείται η ανάγκη προστασίας των εννόμων συμφερόντων του εργοδότη που επεκτείνονται από την απλή διασφάλιση των απορρήτων στοιχείων της επιχείρησης, την πρόληψη ευθυνών του από παράνομες ιδιωτικές συμπεριφορές των μισθωτών μέχρι την αξίωσή του να μη χρησιμοποιείται ο χρόνος εργασίας για προσωπικούς λόγους⁸¹. Όπως επανειλημμένως δέχεται το ΔΕΕ⁸² τα θεμελιώδη δικαιώματα στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα, τα οποία κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη, δεν αποτελούν απόλυτα προνόμια, αλλά πρέπει να λαμβάνονται υπόψη σε σχέση με τη λειτουργία την οποία επιτελούν στο κοινωνικό σύνολο και να σταθμίζονται με άλλα θεμελιώδη δικαιώματα. Επομένως, επιτρέπεται η επιβολή περιορισμών, υπό την προϋπόθεση ότι, σύμφωνα με το άρθρο 52, παράγραφος 1, του Χάρτη, προβλέπονται από τον νόμο και σέβονται το βασικό περιεχόμενο των θεμελιωδών δικαιωμάτων καθώς και την αρχή της αναλογικότητας. Βάσει της εν λόγω αρχής, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε σκοπούς γενικού συμφέροντος τους οποίους αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων⁸³. Οι περιορισμοί αυτοί πρέπει να μην υπερβαίνουν τα όρια του απολύτως αναγκαίου και η ρύθμιση που συνεπάγεται την επέμβαση, πρέπει να προβλέπει σαφείς και ακριβείς κανόνες που να διέπουν την έκταση και την εφαρμογή του επίμαχου μέτρου. Όσο πιο ευρεία είναι η έκταση της επέμβασης στο δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα τόσο πιο δύσκολο είναι να δικαιολογηθεί με

⁸¹ Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το γενικό κανονισμό προστασίας δεδομένων, σελ. 114.

⁸² ΔΕΕ 1.8.2022, C-184/20, ΟΤ κατά Vyriausioji tarnybinės etikos komisija, EU:C:2022:601, σκέψη 70· ΔΕΕ 22.6.2021, C-439/19, Latvijas Republikas Saeima, EU:C:2021:504, σκέψη 105 και εκεί μνημονευόμενη νομολογία.

⁸³ Σε εθνικό επίπεδο η ανάγκη αυτή προστασίας του εργοδότη αναγνωρίστηκε με την υπ' αριθμόν 1/2017 απόφαση της Ολομέλειας του Αρείου Πάγου, σύμφωνα με την οποία η διασφάλιση της εμπορικής πίστης και η προστασία του εργοδότη από αθέμιτο ανταγωνισμό δικαιολογεί την επεξεργασία προσωπικών δεδομένων σχετικών με την ιδιωτική ζωή. Όμως, ο απόλυτος τρόπος με τον οποίο διατυπώνεται η θέση του Αρείου Πάγου δεν είναι ορθός, γιατί η επαγγελματική ζωή δεν εκμηδενίζει πλήρως την προσωπικότητα του εργαζομένου. Απλώς τίθενται περιορισμοί που προκύπτουν από τις αρχές, οι οποίες πρέπει να εφαρμόζονται για την επεξεργασία προσωπικών δεδομένων και την προστασία του απορρήτου των επικοινωνιών και που επιχειρούν να οριοθετήσουν πότε υπερέχει το στοιχείο της επαγγελματικής ζωής και πότε της ιδιωτικής ζωής. Η τελική κρίση προϋποθέτει εξατομίκευση της κάθε περίπτωσης. Για την εξατομίκευση αυτή κρίσιμο μέτρο είναι ο βαθμός σύνδεσης της επαγγελματικής και της ιδιωτικής ζωής.

βάση την αρχή της αναλογικότητας, καθώς το πλήγμα φαίνεται να προσεγγίζει ή και να αφορά στην ουσία του δικαιώματος⁸⁴. Ο ενωσιακός δικαστής, σε πολλές υποθέσεις, έχει καταστήσει σαφές ότι το άρθρο 8 του Χάρτη επιτελεί συγκεκριμένο ρόλο στην κοινωνία, ο οποίος συνίσταται στην προστασία της ιδιωτικής ζωής του ατόμου από αθέμιτες παρεμβάσεις κι όχι στη διευκόλυνση ή τη συγκάλυψη παράνομων πράξεων.

III. Όροι και προϋποθέσεις για τον έλεγχο των ηλεκτρονικών επικοινωνιών των εργαζομένων στο χώρο εργασίας τους

Όπως σημειώθηκε παραπάνω, το βασικό ζήτημα, το οποίο ανακύπτει στην περίπτωση επεξεργασίας των ηλεκτρονικών δεδομένων των εργαζομένων, έγκειται στην αξιολόγηση του απαραίτητου και αναγκαίου χαρακτήρα της. Για το ζήτημα αυτό κατατοπιστική είναι η νομολογία του ΕΔΔΑ, που επιχειρεί, μέσα από αποφάσεις του, να σταθμίσει τα συγκρουόμενα έννομα αγαθά και να προσφέρει ισορροπημένες λύσεις. Οι λύσεις αυτές ενδιαφέρουν και στο πλαίσιο εφαρμογής ενωσιακών κανόνων, καθώς, μολονότι η ΕΣΔΑ δεν συνιστά - ενόσω η Ένωση δεν έχει προσχωρήσει σε αυτήν - νομική πράξη τυπικώς ενταγμένη στην έννομη τάξη της Ένωσης, ωστόσο δεν πρέπει να παραγνωρίζεται αφενός ότι, όπως επιβεβαιώνει το άρθρο 6παρ.3 ΣΕΕ, τα κατοχυρωμένα στην ΕΣΔΑ θεμελιώδη δικαιώματα αποτελούν τμήμα του δικαίου της Ένωσης ως γενικές αρχές και αφετέρου, ότι όπως ορίζει το άρθρο 52παρ.3 ΧΘΔΕΕ, τα περιεχόμενα στον Χάρτη δικαιώματα τα οποία αντιστοιχούν σε δικαιώματα διασφαλιζόμενα από την ΕΣΔΑ, έχουν την ίδια έννοια και την ίδια εμβέλεια με εκείνες που τους αποδίδει η εν λόγω Σύμβαση⁸⁵. Είναι γεγονός ότι το άρθρο 8 του Χάρτη «βασίστηκε», μεταξύ άλλων, και στο άρθρο 8 της ΕΣΔΑ για το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, μολονότι κατά καιρούς λαμβάνουν χώρα διακηρύξεις περί του αντιθέτου⁸⁶. Άλλωστε προφανής είναι η αντιστοιχία μεταξύ των διατάξεων των άρθρων 7 ΧΘΔ και 8 ΕΣΔΑ, με αποτέλεσμα να γίνεται δεκτό ότι οι

⁸⁴ Βλ. Σαρμά, σε: Σαχπεκίδου/Ταγαρά, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, 2020, σελ. 127

⁸⁵ ΔΕΕ 26.2.2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, σκέψη 44, και εκεί μνημονευόμενη νομολογία· ΔΕΕ 20.3.2018 και της 20ής Μαρτίου 2018, Meni, C-524/15, EU:C:2018:197, σκέψη 22.

⁸⁶ ΔΕΕ 21.12.2016, συνεκδικ. υποθ. C-203/15, Tele2 Sverige, και C-698/15, Watson κ.ά., EU:C:2016:970, σκ.129. Βλ. και I. CAMERON, «Balancing data protection and law enforcement needs: Tele2 Sverige and Watson», Common Market Law Review 2017.1467, 1492, όπου διατυπώνεται η άποψη ότι η αναγνώριση της μη αντιστοιχίας του άρθρου 8 του Χάρτη με κάποια διάταξη της ΕΣΔΑ αποτελεί μία «δήλωση ανεξαρτησίας» του ΔΕΕ από το ΕΔΔΑ.

περιορισμοί που δύνανται να επιβληθούν στην πρώτη περίπτωση, είναι οι ίδιοι με εκείνους που επιτρέπονται από τη δεύτερη παράγραφο του άρθρου 8, σύμφωνα με την οποία «Δεν επιτρέπεται να υπάρξει επέμβαση δημόσιας αρχής στην άσκηση του δικαιώματος αυτού, εκτός εάν η επέμβαση αυτή προβλέπεται από το νόμο και αποτελεί μέτρο το οποίο, σε μια δημοκρατική κοινωνία, είναι αναγκαίο για την εθνική ασφάλεια, τη δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής ή την προστασία των δικαιωμάτων και ελευθεριών άλλων»⁸⁷.

Από τις αποφάσεις που έχουν εκδοθεί από το ΕΔΔΑ σχετικά με το προκείμενο ζήτημα, γνωστότερες είναι οι αποφάσεις Niemietz κατά Γερμανίας (αποφ. 16-2-1992), Hollford κατά Ηνωμένου Βασιλείου (απόφ. 27.6.1997), Compland κατά Ηνωμένου Βασιλείου (απόφ. 3-4-2002), Barbulescu κατά Ρουμανίας (απόφ. 7-9-2017)⁸⁸. Η τελευταία είναι και πιο συναφής σε θέματα εργασιακών σχέσεων, γιατί αφορά συγκεκριμένη υποχρέωση εργαζομένου να μην αφιερώνει επαγγελματικό χρόνο για προσωπικές επικοινωνίες. Η υπόθεση αφορούσε παρακολούθηση ηλεκτρονικού ταχυδρομείου στο yahoo.messenger που είχε τεθεί στη διάθεση του εργαζομένου και το χρησιμοποιούσε και για προσωπικούς λόγους.

Κοινός πάντως τύπος των ανωτέρω αποφάσεων είναι η διαπίστωση παραλείψεων από την πλευρά του εργοδότη κατά την επεξεργασία προσωπικών δεδομένων. Σε όλες τις υποθέσεις αυτές, το ΕΔΔΑ δέχτηκε ότι η προστασία του ιδιωτικού βίου δεν περιορίζεται στην καθαρά ιδιωτική ζωή, αλλά επεκτείνεται και στην επαγγελματική ζωή. Ειδικότερα, στην υπόθεση Niemietz, το Δικαστήριο σημειώνει ότι είναι αδύνατο να προσδιορίσουμε την ιδιωτική ζωή και έτσι εντάσσει σε αυτή «...το δικαίωμα του προσώπου να αναπτύσσει σχέσεις με τους συνανθρώπους...» (σκ. 29). Ακόμα, στις εν λόγω αποφάσεις, αναγνωρίζεται η δυσκολία διάκρισης μεταξύ επαγγελματικής ζωής και ιδιωτικής χρήσης μέσων επικοινωνίας της επιχείρησης. Ενώ δεν αμφισβητείται το δικαίωμα ελέγχου του εργοδότη των επικοινωνιών του εργαζομένου, επισημαίνεται από το ΕΔΔΑ ότι αυτό δεν είναι ανέλεγκτο. Έτσι, γίνεται μεν δεκτή η δυνατότητα επεξεργασίας για νόμιμο σκοπό, αλλά και πάλι ελέγχεται ο τρόπος και η έκταση επεξεργασίας. Σε όλες τις περιπτώσεις κρίσιμο στοιχείο που βάρυνε στην κρίση του ΕΔΔΑ ήταν η έλλειψη ενημέρωσης του ενδιαφερομένου με

⁸⁷ Βλ. Τάκη, σε: Σαγκρεκίδου/Ταγαρά, Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, 2020, σελ. 86.

⁸⁸ Διαθέσιμες όλες σε <https://hudoc.echr.coe.int>.

σαφή τρόπο (σκοπός, έκταση, φύση). Βαρύνουσα σημασία για την στάθμιση των νομίμων συμφερόντων εργοδότη και εργαζομένου είχε η διάταξη του άρθρου 8 της ΕΣΔΑ, με την οποία κατοχυρώνεται το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής καθώς και της αλληλογραφίας κάθε προσώπου. Υπό το φως του εν λόγω δικαιώματος, οι εθνικές ρυθμίσεις κάθε κράτους πρέπει -κατά το ΕΔΔΑ- να εξασφαλίζουν ισορροπημένη στάθμιση μεταξύ των συμφερόντων αφενός του εργοδότη, αφετέρου του εργαζομένου και να διασφαλίζουν έναν πυρήνα ιδιωτικής ζωής του τελευταίου στο χώρο εργασίας.

Σε εθνικό επίπεδο, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα κλήθηκε, κατά το παρελθόν, να λάβει θέση ως προς την νομιμότητα ενός πληροφοριακού συστήματος, το οποίο καθιστά δυνατή την πρόσβαση του εργοδότη στους υπολογιστές των εργαζομένων και ιδίως των ηλεκτρονικών επικοινωνιών των τελευταίων και την καταγραφή των διαδικτυακών τόπων που επισκέπτονται. Με την υπ' αριθμόν 61/2004 απόφασή της αποφάνθηκε ότι η συλλογή και η επεξεργασία δεδομένων που αφορούν τις κλήσεις και γενικά τις επικοινωνίες (στις οποίες συμπεριλαμβάνεται το ηλεκτρονικό ταχυδρομείο) στο χώρο εργασίας, επιτρέπεται εφόσον είναι απολύτως αναγκαία για την οργάνωση και τον έλεγχο της διεκπεραίωσης της συγκεκριμένης εργασίας ή του κύκλου εργασιών και ιδίως τον έλεγχο των δαπανών. Τα στοιχεία της επικοινωνίας που καταχωρίζονται, πρέπει να περιορίζονται στα απολύτως απαραίτητα και πρόσφορα δεδομένα για την επίτευξη των σκοπών αυτών. Σε καμία περίπτωση δεν επιτρέπεται η καταχώρηση και επεξεργασία του συνόλου των στοιχείων της επικοινωνίας ή στοιχείων από το περιεχόμενό τους, τα οποία δεν επιτρέπεται να συλλεχθούν παρά μόνο με άδεια της δικαστικής αρχής και εφόσον τούτο επιβάλλεται για λόγους εθνικής ασφάλειας ή για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Επομένως, η πρόσβαση και η καταγραφή στοιχείων ηλεκτρονικής επικοινωνίας των εργαζομένων της εταιρείας δεν είναι νόμιμη και τέτοια στοιχεία δεν μπορούν να χρησιμοποιηθούν για τον έλεγχο της συμπεριφοράς των εργαζομένων.

Επίσης με την υπ' αριθμόν 34/2018 απόφασή της η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα⁸⁹ έδωσε απάντηση σε μία σειρά από ερωτήματα που συνεχονται άμεσα με το επιτρεπτό της επεξεργασίας των δεδομένων ενός εργαζομένου στο πλαίσιο εσωτερικού ελέγχου. Συγκεκριμένα, ο έλεγχος υπολογιστή

⁸⁹ Url: <https://www.taxheaven.gr/circulars/28598/apdpx-ar-34-2018>.

και των αποθηκευμένων, ηλεκτρονικώς, εγγράφων που ανήκουν στην εταιρεία, δεν είναι αυτόματα νόμιμος. Και στην περίπτωση αυτή γίνεται στάθμιση, κατά την απόφαση, αφενός της νόμιμης προσδοκίας της ιδιωτικής ζωής του εργαζομένου στο χώρο εργασίας, που δεν αίρεται από το γεγονός ότι χρησιμοποιεί εξοπλισμό της εταιρείας και αφετέρου της ανάγκης εύρυθμης λειτουργίας της επιχείρησης (ικανοποίηση εννόμου συμφέροντος του εργοδότη). Ο εργοδότης πρέπει να αποδεικνύει κάποιον νόμιμο λόγο επεξεργασίας των δεδομένων (π.χ. υποψία διάπραξης αξιόποινης πράξης, αθέμιτος ανταγωνισμός), ~~π~~ο οποίος πρακτικά συνδέεται και με το δικαίωμα ελέγχου από τον εργοδότη της υποχρέωσης πίστης του εργαζομένου (υποχρέωση παροχής πληροφοριών από τον εργαζόμενο, έλεγχο διαρροής εμπιστευτικών πληροφοριών). Τα παραπάνω στοιχεία συγκροτούν και συνθέτουν το «αναγκαίον» της επεξεργασίας. Επιπλέον για τον επιτρεπτό χαρακτήρα της επεξεργασίας, ο εργοδότης πρέπει να ενημερώνει τον εργαζόμενο για την επικείμενη επεξεργασία, η οποία, καταρχάς, θα πρέπει να γίνεται παρουσία του και να μη θίγονται θεμελιώδη δικαιώματα του εργαζομένου. Αυτή η προϋπόθεση σημαίνει, κατά την απόφαση της Α.Π.Δ.Π.Χ., ότι η επεξεργασία πρέπει να γίνεται με αντικειμενικούς όρους και διακριτικότητα. Το δικαίωμα της επεξεργασίας δεδομένων εν αγνοία του εργαζομένου δεν αποκλείεται *argiōi* σε ορισμένες, όλως εξαιρετικές, περιπτώσεις, εφόσον αυτό δεν αντίκειται στην εθνική νομοθεσία και έχει τηρηθεί το αναγκαίο μέτρο. Συμπληρωματικώς, αναγνωρίζεται στον εργοδότη το δικαίωμα να αρνηθεί προσωρινή πρόσβαση του εργαζομένου στον προσωπικό υπολογιστή ή και να προβεί σε προσωρινή απενεργοποίηση του υπολογιστή, προκειμένου να καταστεί εφικτή η παρουσία του εργαζομένου. Αυτό, κατά την παραπάνω απόφαση της ΑΠΔΠΧ, συνιστά λιγότερο επαχθές μέτρο και πρέπει να προτιμάται, γιατί παρέχει και μεγαλύτερη ασφάλεια στον εργοδότη.

Ιδιαίτερη σημασία έχει το δικαίωμα του εργοδότη να καταστήσει γνωστό εκ των προτέρων στον εργαζόμενο ότι απαγορεύεται η χρησιμοποίηση του ηλεκτρονικού υπολογιστή της εταιρείας για προσωπικά δεδομένα του εργαζομένου. Η συναίνεση αυτή πρέπει να είναι σαφής. Ο εργαζόμενος δεν έχει αξίωση για ιδιωτική χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου στο χώρο εργασίας και αυτό δέχτηκε πρόσφατα και το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου⁹⁰. Αξίωση αποκτά ο εργαζόμενος μόνον όταν ο εργοδότης ρητά ή σιωπηρά έχει επιτρέψει την

⁹⁰ ΕΔΔΑ 12.1.2016 – 6149/08. Βλ. και Ιγγλεζάκη, ΔιΜΕΕ 2005, 57.

ιδιωτική χρήση. Σιωπηρή συναίνεση προκύπτει π.χ. από το γεγονός ότι ο εργοδότης γνωρίζει ότι ο εργαζόμενος επανειλημμένα κάνει χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου για προσωπικούς σκοπούς και ανέχεται τη χρήση αυτή⁹¹.

Εάν ο εργοδότης έχει επιτρέψει στο προσωπικό την ιδιωτική (προσωπική) χρήση των ηλεκτρονικών μέσων επικοινωνίας που του έχει παραχωρήσει στο πλαίσιο της εργασιακής σχέσης, τότε βρίσκουν εφαρμογή εκτός από το νόμο 4624/2019, και οι διατάξεις για την προστασία του απορρήτου των επικοινωνιών, οι οποίες, προς διασφάλιση του απορρήτου των επικοινωνιών και της προστασίας της ιδιωτικής ζωής των πολιτών, περιορίζουν σημαντικά τη δυνατότητα επεξεργασίας προσωπικών δεδομένων⁹². Ως γενικός κανόνας ισχύει η απαγόρευση ελέγχου του περιεχομένου των ηλεκτρονικών μηνυμάτων που αποστέλλει ή λαμβάνει ο εργαζόμενος χρησιμοποιώντας την επαγγελματική ηλεκτρονική διεύθυνση της επιχείρησης. Η απαγόρευση αφορά γενικά τα ηλεκτρονικά μηνύματα, καθόσον μία διάκριση -στην περίπτωση που έχει επιτραπεί στον εργαζόμενο η ιδιωτική χρήση- σε μηνύματα υπηρεσιακά και προσωπικά είναι πρακτικά αδύνατη. Ακόμα και σε περίπτωση απουσίας του εργαζόμενου από το χώρο εργασίας λόγω ασθένειας ή για άλλο λόγο δεν επιτρέπεται στον εργοδότη να ελέγξει το περιεχόμενο των ηλεκτρονικών μηνυμάτων που έχει λάβει ή αποστείλει ο εργαζόμενος χρησιμοποιώντας την ηλεκτρονική διεύθυνση της επιχείρησης⁹³. Η απαγόρευση ελέγχου εκτείνεται και στις ιστοσελίδες που ο εργαζόμενος επισκέπτεται κάνοντας χρήση της διαδικτυακής σύνδεσης που του παρέχει ο εργοδότης του. Ιδιαίτερο ενδιαφέρον από νομικής απόψεως εμφανίζουν οι επισκέψεις των εργαζομένων σε ιστοσελίδες κοινωνικής δικτύωσης (π.χ. facebook, twitter), όπου πέραν από πληροφορίες, πολλές φορές αναρτούν και φωτογραφικά ή ηχητικά δεδομένα από τον τόπο εργασίας τους, κοινοποιώντας τα σε μεγάλο αριθμό φιλικών ή απλώς γνωστών τους προσώπων⁹⁴.

⁹¹ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 987, 99.

⁹² Προσωπικά δεδομένα που καλύπτονται από το απόρρητο συνιστούν την αυστηρότερη κατηγορία απαγόρευσης επεξεργασίας προσωπικών δεδομένων. Ο αποχαρακτηρισμός από το απόρρητο οδηγεί την ένταξη της προστασίας των προσωπικών δεδομένων στις γενικές διατάξεις του γενικού κανονισμού προστασίας δεδομένων. Σχετικές δεν την παραπάνω διαβάθμιση είναι και η προβλεπόμενη στο νόμο αδυναμία χρησιμοποίησης, σε οποιοδήποτε δική, αποκτηθέντων δεδομένων κατά παράβαση του απορρήτου σύμφωνα με το άρθρο 19 του Συντάγματος καθώς και η αδυναμία επίκλησης των παρανόμως αποκτηθέντων αποδεικτικών μέσων κατά το άρθρο 9Α του Συντάγματος. Βλ. Κουκιάδη, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το γενικό κανονισμό προστασίας δεδομένων, σελ. 124.

⁹³ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 988, 101.

⁹⁴ Wolfgang Däubler, Internet und Arbeitsrecht, Web 2.0, Social Media und Crowdwork, σελ. 167επ.

Εναλλακτικώς στην ακώλυτη ιδιωτική χρήση των μέσων επικοινωνίας της εταιρείας από τους εργαζομένους, θα μπορούσε να επιβάλλεται η χρήση μιας προσωπικής ηλεκτρονικής διεύθυνσης ή ο χαρακτηρισμός - διαγραφή των μηνυμάτων, όταν αυτά είναι προσωπικά. Επίσης, η τεχνολογία παρέχει στον εργοδότη τη δυνατότητα είτε να αποκλείσει την πρόσβαση του μισθωτού σε ορισμένες ιστοσελίδες με παράνομο ή ενγένει αθέμιτο περιεχόμενο είτε (επειδή δεν είναι ευχερές να παρακολουθεί την καθημερινή δημιουργία νέων αθέμιτων ιστοσελίδων) να παράσχει πρόσβαση μόνον σε ορισμένες ιστοσελίδες που συνδέονται με τις ανάγκες της εργασίας του μισθωτού. Σε μια τέτοια περίπτωση, θα πρέπει: πρώτον, να τηρήσει την αρχή της ίσης μεταχείρισης, δηλαδή να μην προβεί σε αυθαίρετες διαφοροποιήσεις μεταξύ των μισθωτών και δεύτερον, να μην προσβάλλει την προσωπικότητα του μισθωτού με αθέμιτη επιλογή των προσβάσιμων ιστοσελίδων, λ.χ. επιτρέποντας την πρόσβαση στην ιστοσελίδα ενός μόνο πολιτικού κόμματος ή μιας εφημερίδας⁹⁵. Σε περίπτωση που ο εργοδότης δεν καθορίσει τις μη προσβάσιμες ιστοσελίδες, νομιμοποιείται να καταγράψει με απρόσωπο τρόπο τις ιστοσελίδες που επισκέπτονται οι μισθωτοί του. Μόνον εάν διαπιστώσει ότι υπάρχει επίσκεψη σε ιστοσελίδα, την οποία έχει απαγορεύσει (είτε εξατομικευμένα είτε περιγραφικά), θα μπορεί να προχωρήσει στον εντοπισμό του συγκεκριμένου μισθωτού και να λάβει μέτρα σε βάρος του, αφού πρώτα του παράσχει το δικαίωμα ακροάσεως. Επίσης, μέτρα θα μπορεί να λάβει, εάν ένας εργαζόμενος αναλώνει σημαντικό μέρος του χρόνου εργασίας του στο διαδίκτυο για λόγους άσχετους με την εργασία του. Στην περίπτωση αυτή, ορθό θα ήταν ο έλεγχος να περιορίζεται απλώς στη διαπίστωση του χρόνου που καταναλώνει ο εργαζόμενος στο διαδίκτυο και να μην επεκτείνεται ειδικότερα στο περιεχόμενο των ιστοσελίδων που επισκέπτεται⁹⁶.

Ζήτημα επίσης ανακύπτει στην περίπτωση που ο εργαζόμενος παραλείψει να χαρακτηρίσει κάποιο μήνυμά του ως προσωπικό ή υπηρεσιακό. Έχει ορθώς υποστηριχθεί η άποψη⁹⁷ ότι σε μια τέτοια περίπτωση εύλογα τίθεται ένα τεκμήριο υπέρ του υπηρεσιακού χαρακτήρα του μηνύματος. Το τεκμήριο αυτό δικαιολογείται για δύο λόγους: Πρώτον, γιατί εύλογα αναμένει κανείς η πλειοψηφία των μηνυμάτων που αποστέλλει και λαμβάνει ο εργαζόμενος στο χώρο εργασίας του, να έχουν υπηρεσιακό

⁹⁵ Παπαϊωάννου, Ο έλεγχος από τον εργοδότη της ηλεκτρονικής αλληλογραφίας και της ενασχόλησης του μισθωτού με το διαδίκτυο, ΕΕργΔ 2006, σελ. 730.

⁹⁶ Παπαϊωάννου, ο.π., ΕΕργΔ 2006, σελ. 730.

⁹⁷ Παπαϊωάννου, ό.π., ΕΕργΔ 2006, σελ. 730.

χαρακτήρα. Δεύτερον, γιατί την πρωτοβουλία του χαρακτηρισμού την έχει ο εργαζόμενος και άρα αυτός θα πρέπει να «χρεωθεί» την τυχόν παράλειψή του, υπό την αυτονόητη βέβαια προϋπόθεση ότι θα έχει ενημερωθεί πλήρως και με σαφήνεια για την σχετική υποχρέωσή του.

Ενώ δεν επιτρέπεται ο έλεγχος του περιεχομένου των ηλεκτρονικών μηνυμάτων και των ιστοσελίδων που επισκέπτεται ο εργαζόμενος στο διαδίκτυο, αντίθετα, ως προς την καταγραφή και επεξεργασία εξωτερικών στοιχείων της επικοινωνίας του εργαζόμενου, δεν υφίσταται απαγόρευση. Ο εργοδότης, εφόσον έχει επιτρέψει στους εργαζόμενους την ιδιωτική χρήση των ηλεκτρονικών μέσων επικοινωνίας της επιχείρησης, έχει ένα εύλογο συμφέρον να πληροφορείται σε ποια έκταση ο εργαζόμενος κάνει χρήση για προσωπικούς σκοπούς των μέσων αυτών σε βάρος του χρόνου εργασίας του. Όμως, η καταγραφή και επεξεργασία των στοιχείων αυτών (όπως χρόνος αποστολής και λήψης των μηνυμάτων, στοιχεία ως προς τους αποστολείς και αποδέκτες των μηνυμάτων, καταγραφή των διαδικτυακών τόπων που επισκέπτεται ο εργαζόμενος συχνότητα χρήσης του διαδικτύου και του ηλεκτρονικού ταχυδρομείου κλπ.) υπόκειται σε περιορισμούς, όπως προκύπτει και από την υπ' αριθμόν 61/2004 απόφαση της Α.Α.Π.Δ.Π.Χ.. Κι εδώ οι αρχές του σκοπού και της αναλογικότητας έχουν καθοριστική σημασία για τον προσδιορισμό των θεμιτών ορίων νόμιμης συλλογής και επεξεργασίας στοιχείων της ηλεκτρονικής επικοινωνίας του εργαζόμενου.

Ωστόσο, και στην περίπτωση που ο εργοδότης έχει απαγορεύσει στον εργαζόμενο την χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου της επιχείρησης για ιδιωτικούς σκοπούς, η νομιμότητα του ελέγχου του διαδικτύου και του ηλεκτρονικού ταχυδρομείου από τον εργοδότη κρίνεται βάσει των διατάξεων του Γ.Κ.Π.Δ. και του νόμου 4624/2019. Βασικά ο εργοδότης έχει δικαίωμα να πληροφορείται το περιεχόμενο κάθε υπηρεσιακής ηλεκτρονικής αλληλογραφίας, όπως έχει δικαίωμα να πληροφορείται το περιεχόμενο κάθε είδους υπηρεσιακής αλληλογραφίας. Έτσι μπορεί να αξιώσει από τον εργαζόμενο να του θέσει υπόψη όλα τα υπηρεσιακά ηλεκτρονικά μηνύματα που έχει αποστείλει ή έχει λάβει. Ο έλεγχος της όλης εργασιακής διαδικασίας και των αποτελεσμάτων της ανήκει στο διευθυντικό του δικαίωμα. Επιφυλάξεις ως προς την νομιμότητα του ελέγχου εγείρονται, όταν αυτός διεξάγεται χωρίς τη γνώση και την συνεργασία του εργαζόμενου. Στην περίπτωση αυτή, ένας δειγματοληπτικός έλεγχος από τον εργοδότη των ηλεκτρονικών μηνυμάτων του εργαζόμενου και της πρόσβασης στο διαδίκτυο θεωρείται επιτρεπτός. Αντίθετα,

δεν θεωρείται επιτρεπτός ο συνεχής και αδιάκοπος για μεγάλο χρονικό διάστημα έλεγχος, χωρίς τη γνώση του εργαζόμενου. Ένας τέτοιος συστηματικός έλεγχος παραβιάζει την αρχή της αναλογικότητας και συνιστά παράνομη επέμβαση στην προσωπικότητα του⁹⁸.

Στην περίπτωση, πάντως, που η χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου της επιχείρησης έχει επιτραπεί αποκλειστικά και μόνο για υπηρεσιακούς σκοπούς, απαγορεύεται ο έλεγχος από τον εργοδότη μηνυμάτων που είναι σαφές ότι πρόκειται για προσωπικά μηνύματα του εργαζόμενου. Η ανάγνωση της προσωπικής ηλεκτρονικής αλληλογραφίας του εργαζόμενου συνιστά βαριά προσβολή της ιδιωτικής του ζωής (άρθρ. 9παρ.1 Συντ., 8 ΕΣΔΑ) και γενικότερα της προσωπικότητας του. Συνεπώς, δεν μπορεί να νομιμοποιηθεί για το λόγο ότι η ηλεκτρονική επικοινωνία για προσωπικούς σκοπούς γίνεται στο χώρο εργασίας και με τη χρήση ηλεκτρονικών μέσων που έχει διαθέσει ο εργοδότης. Ο εργαζόμενος έχει αξίωση για προστασία της ιδιωτικής του ζωής και στο χώρο εργασίας⁹⁹. Το δικαίωμα της ιδιωτικής ζωής, όπως επισημαίνει το ΕΔΔΑ, συμπεριλαμβάνει το δικαίωμα κάθε ανθρώπου να συνάπτει και να αναπτύσσει σχέσεις με άλλους ανθρώπους και δε συντρέχει κανένας λόγος να αποκλείσουμε από την έννοια της ιδιωτικής ζωής τις επαγγελματικές δραστηριότητες και τις εργασιακές σχέσεις, δεδομένου ότι η πλειονότητα των ανθρώπων έχουν μία σημαντική, αν όχι την μεγαλύτερη, ευκαιρία ανάπτυξης των σχέσεων τους στο χώρο εργασίας¹⁰⁰. Όπως εύστοχα και παραστατικά επισημαίνεται, οι εργαζόμενοι «δεν εγκαταλείπουν το δικαίωμά τους για προστασία της ιδιωτικής του ζωής και προστασία των προσωπικών δεδομένων τους κάθε πρωί στην είσοδο του τόπου εργασίας»¹⁰¹. Η εύλογη αυτή προσδοκία προστασίας της ιδιωτικής τους ζωής και του απορρήτου των επικοινωνιών στον τόπο εργασίας δεν αίρεται από το γεγονός ότι χρησιμοποιούν εξοπλισμό, συσκευές επικοινωνιών και οποιεσδήποτε άλλες επαγγελματικές εγκαταστάσεις του εργοδότη¹⁰².

Τέλος, ακόμα και αν ο εργοδότης έχει απαγορεύσει την χρήση του διαδικτύου και γενικότερα των ηλεκτρονικών μέσων επικοινωνίας για ιδιωτικούς σκοπούς, δε σημαίνει ότι επιτρέπεται η χρήση από την πλευρά του κάθε μέσου επιτήρησης και ελέγχου των ιδιωτικού χαρακτήρα επικοινωνιών των εργαζομένων. Και στην

⁹⁸ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 989, 104.

⁹⁹ ΟΛΑΠ 1/2017, ΤΝΠ ΝΟΜΟΣ.

¹⁰⁰ ΕΔΔΑ αποφ. 16.12.1992, Niemietz κατά Γερμανίας.

¹⁰¹ Γνώμη 8/2001 της Ομάδας Εργασίας του άρθρου 29.

¹⁰² Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 990, 106.

περίπτωση αυτή ο εργαζόμενος έχει αξίωση σεβασμού της ιδιωτικής του ζωής, η δε επέμβαση στο δικαίωμά του αυτό δεν επιτρέπεται, εάν ο εργαζόμενος δεν έχει προηγουμένως ενημερωθεί για το είδος και την έκταση της παρακολούθησης της ηλεκτρονικής του αλληλογραφίας, η οποία (παρακολούθηση) σε κάθε περίπτωση θα πρέπει να τηρεί την αρχή της αναλογικότητας¹⁰³.

IV. Ποινική ευθύνη εργοδότη κατά την επεξεργασία ηλεκτρονικών δεδομένων του εργαζομένου στο πλαίσιο εσωτερικών ερευνών

Το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου στην υπόθεση Halford κατά Ηνωμένου Βασιλείου¹⁰⁴ αποφάνθηκε ότι η υποκλοπή τηλεφωνικής επικοινωνίας υπαλλήλου συνιστά παράβαση του άρθρου 8 της ΕΣΔΑ. Το Δικαστήριο υπάγει στην έννοια της αλληλογραφίας, κατά το άρθρο 8 της ΕΣΔΑ, όχι μόνο την περίπτωση της επικοινωνίας με επιστολές αλλά και την ηλεκτρονική αλληλογραφία που διενεργείται από το χώρο εργασίας και με τα τεχνικά μέσα που παρέχει ο εργοδότης στον εργαζόμενο. Η χρήση κρυφών συσκευών, με σκοπό την υποκλοπή ιδιωτικών συνδιαλέξεων αποτελεί επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής ασχέτως του περιεχομένου της συνδιάλεξης. Το άρθρο 8 της ΕΣΔΑ επιβάλλει την προστασία των τηλεφωνικών συνδιαλέξεων, ακόμα και αυτές που έχουν επαγγελματικό περιεχόμενο και γίνονται μέσω συσκευής που βρίσκεται στο γραφείο της επιχείρησης. Ίδιας εμβέλειας είναι η προστασία που παρέχουν οι διατάξεις των άρθρων 7, 8 ΧΘΔΕΕ βάσει της επιταγής της ομοιογένειας που απορρέει από το άρθρο 52παρ.3 του Χάρτη.

Σε εθνικό επίπεδο, ο έλεγχος και η παρακολούθηση του περιεχομένου της ηλεκτρονικής αλληλογραφίας του εργαζομένου δεν παραβιάζει μόνο τη νομοθεσία για την προστασία των προσωπικών δεδομένων αλλά και το απόρρητο της επικοινωνίας, η συνταγματική προστασία (άρθρο 19παρ.1 Συντ) του οποίου ολοκληρώνεται με τη θέσπιση ποινικών κυρώσεων σε βάρος των παραβατών. Σε περίπτωση που ο εργοδότης, παρακάμπτοντας τους ως άνω όρους και προϋποθέσεις για τον επιτρεπτό έλεγχο των ηλεκτρονικών επικοινωνιών των εργαζομένων στο χώρο εργασίας τους, λάβει γνώση των ηλεκτρονικών δεδομένων τους χωρίς τη συναίνεσή τους, τίθεται ζήτημα εφαρμογής των ποινικών διατάξεων στις οποίες τυποποιούνται οι προσβολές

¹⁰³ Βλ. Ζερδελή, Εργατ.Δικ., εκδ. 2019, σελ. 991, 107.

¹⁰⁴ Διαθέσιμη σε <https://hudoc.echr.coe.int>.

του απορρήτου των επικοινωνιών και ιδίως των άρθρων 370παρ.2-1 και 370Επαρ.1 ΠΚ¹⁰⁵.

Σύμφωνα με τη διάταξη του άρθρου 370 ΠΚ «1. Όποιος αθέμιτα και με σκοπό να λάβει γνώση του περιεχομένου τους ανοίγει ξένη κλειστή επιστολή ή άλλο κλειστό έγγραφο ή παραβιάζει κλειστό χώρο, στον οποίο είναι αυτά φυλαγμένα, ή με οποιονδήποτε τρόπο εισχωρεί σε ξένα απόρρητα διαβάζοντας ή αντιγράφοντας ή αποτυπώνοντας με άλλο τρόπο επιστολή ή άλλο έγγραφο τιμωρείται με φυλάκιση έως δύο έτη ή χρηματική ποινή. 2. Με την ποινή της προηγούμενης παραγράφου τιμωρείται και όποιος αθέμιτα αποκτά πρόσβαση σε ηλεκτρονικό μήνυμα ή ηλεκτρονική αλληλογραφία άλλου.», ενώ σύμφωνα με το άρθρο 370^Ε ΠΚ «1. Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών». Με την πρώτη διάταξη, όπως τέθηκε υπό τον νέο Ποινικό Κώδικα, επιδιώχθηκε ο εκσυγχρονισμός του άρθρου 370 ΠΚ μέσω της διεύρυνσης της αξιόποινης συμπεριφοράς, ώστε το έγκλημα που τυποποιείται στην παρ. 1, να τιμωρείται πλέον με τη διάταξη της παρ. 2, όταν τελείται με αθέμιτη πρόσβαση σε ηλεκτρονικό μήνυμα ή ηλεκτρονική αλληλογραφία άλλου. Δηλαδή διευρύνθηκε η εγκληματική συμπεριφορά της παρ.1 ώστε να καταλαμβάνει ρητά πλέον και την παραβίαση του απορρήτου των ηλεκτρονικών μηνυμάτων συγκεκριμένου ατόμου, κατ' αναλογία με όσα ισχύουν για τα απόρρητα που είναι φυλαγμένα σε κλειστό χώρο (παρ.1). Με τη δεύτερη διάταξη του άρθρου 370Επαρ.1 ΠΚ τέθηκε σε εφαρμογή το άρθρο 3 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο¹⁰⁶ και αποβλέπει στην προστασία των δεδομένων που διαβιβάζονται μέσω υπολογιστών με μη δημόσιο τρόπο. Κρίσιμο στοιχείο για την κατάφαση ή μη του στοιχείου «της μη δημοσιότητας των διαβιβάσεων» είναι αυτή καθαυτή η διαδικασία

¹⁰⁵ Φιλόπουλος, Η ποινική προστασία των τηλεπικοινωνιών – Μια πρώτη ερμηνευτική προσέγγιση των βασικών διατάξεων, ΠοινΔνη 2021, σελ. 483.

¹⁰⁶ Ειδικότερα σύμφωνα με το άρθρο αυτό «Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η υποκλοπή διά τεχνικών μέσων μη δημοσίων διαβιβάσεων δεδομένων υπολογιστή από και προς ή εντός ενός συστήματος υπολογιστή, περιλαμβανομένων και των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστή στο οποίο ευρίσκονται αυτά τα δεδομένα υπολογιστών, όταν αυτή διαπράττεται από πρόθεση. Ένα Συμβαλλόμενο Μέρος μπορεί να θέσει ως προϋπόθεση της διάπραξης του εγκλήματος την αθέμιτη πρόθεση, ή την επίτευξη σύνδεσης ενός συστήματος υπολογιστή με ένα άλλο σύστημα υπολογιστή».

διαβίβασης των δεδομένων και όχι η φύση και το περιεχόμενο των διαβιβαζόμενων δεδομένων¹⁰⁷.

Η έννοια των δεδομένων στις παραπάνω διατάξεις δεν περιορίζεται στα προσωπικά δεδομένα κατά την έννοια του άρθρου 4παρ.1 του ΓΚΠΔ, αλλά περιλαμβάνει όλες τις πληροφορίες που περιλαμβάνονται σε συστήματα αποθήκευσης δεδομένων και κωδικοποιούνται σε αναγνωρίσιμη μορφή, ανεξάρτητα από το εάν και με ποια μορφή υποβάλλονται σε επεξεργασία.¹⁰⁸ Συνεπώς, στην έννοια αυτή περιλαμβάνονται όλα τα αρχεία κειμένου, εικόνας, βίντεο ή άλλα αρχεία που θα μπορούσαν να είναι σχετικά με μια εσωτερική έρευνα¹⁰⁹. Δεν έχει σημασία εάν τα δεδομένα είναι αποθηκευμένα σε σύστημα επεξεργασίας δεδομένων (φορητός υπολογιστής) ή σε καθαρό μέσο δεδομένων (σκληρός δίσκος, USB stick, CD-ROM). Ως δεδομένα πρέπει να θεωρηθούν και όσα δεν έχουν οικονομική, επιστημονική ή άυλη αξία, όπως λχ. τα ιδιωτικά διασφαλισμένα δεδομένα των εργαζομένων στους υπολογιστές μιας επιχείρησης¹¹⁰. Αθέμιτη πρόσβαση σε δεδομένα συντρέχει όταν ο δράστης αποκτά μη εξουσιοδοτημένη πρόσβαση σ' αυτά¹¹¹. Επομένως, ο δράστης πρέπει να αποκτήσει πραγματικό έλεγχο των δεδομένων υπερβαίνοντας την ασφάλεια πρόσβασης, η οποία μπορεί να γίνει τόσο με την απόκτηση της κατοχής του αρχικού μέσου αποθήκευσης δεδομένων¹¹² όσο και με την αντιγραφή του στο δικό του μέσο αποθήκευσης¹¹³. Έτσι, παραδοσιακά μέτρα που χρησιμοποιούνται κατά τη διενέργεια εσωτερικών ερευνών (κατοχή του αρχικού φορέα αποθήκευσης, κατοπρισμός σκληρών δίσκων, απόσυρση δεδομένων διακομιστή και ανάλυση δεδομένων) εμπίπτουν στο πεδίο εφαρμογής των παραπάνω διατάξεων¹¹⁴. Παρακολούθηση ή αποτύπωση σημαίνει απόκτηση εξουσίας διάθεσης των δεδομένων· η απλή δυνατότητα

¹⁰⁷ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 483.

¹⁰⁸ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 483 Weidemann, σε: BeckOK StGB, §202a πλαγ. 4· πρβλ. επίσης Eisele, σε: Schönke/Schröder, StGB, § 202a- πλαγ. 2 επ.· Hilgendorf, σε: LK StGB, § 202a πλαγ. 7; Kargl, σε: NK StGB, § 202a πλαγ. 4

¹⁰⁹ Schuster σε Knierim/Rübenstahl/Tsambikakis, Internal Investigations, σελ. 317 πλαγ. 127· Rübenstahl/Debus, NZWiSt 2012, σελ. 130.

¹¹⁰ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 476.

¹¹¹ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 477-478, όπου και περαιτέρω ανάλυση.

¹¹² Weidemann σε BeckOK StGB, § 202a Πλαγ. 18.

¹¹³ Fischer, StGB, § 202a πλαγ. 11· Eisele σε Schönke/Schröder, StGB, § 202a πλαγ. 18· Graf σε MüKo StGB, § 202a πλαγ. 50· Kargl σε NK StGB, § 202a πλαγ. 12· Lackner/ Kühn, StGB, §202a πλαγ.5· Schulze-Heiming, Der strafrechtliche Schutz der Computerdaten, σελ. 81επ.

¹¹⁴ Wilkens, Internal Investigations, σελ. 523· Schuster σε Knierim/Rübenstahl/Tsambikakis, Internal Investigations, σελ. 317 πλαγ. 127· Eisele, Compliance und Datenschutzstrafrecht, σελ. 54· Scharnberg, Illegale Internal Investigations, σελ. 193· Rübenstahl/Debus, NZWiSt 2012, σελ. 130.

πρόσβασης δεν αρκεί για την πλήρωση της αντικειμενικής υπόστασης του εγκλήματος¹¹⁵.

Όπως γίνεται δεκτό¹¹⁶, όταν έχει επιτραπεί η χρήση των ηλεκτρονικών μέσων μιας εταιρείας για ιδιωτικούς σκοπούς των εργαζομένων, οι τελευταίοι είναι οι μόνοι που έχουν δικαίωμα να διαθέσουν τα ηλεκτρονικά δεδομένα τους και συνεπώς ο εργοδότης δε δικαιούται να αποκτήσει πρόσβαση σ' αυτά, χωρίς τη συγκατάθεση των εργαζομένων του¹¹⁷. Οι ιδιωτικές συνομιλίες των εργαζομένων εμπίπτουν στο προστατευτικό πεδίο των παραπάνω διατάξεων και επομένως δεν επιτρέπεται στον εργοδότη η παρακολούθηση με τεχνικά μέσα της ηλεκτρονικής αλληλογραφίας και των (μη δημόσιων) ιδιωτικών συνομιλιών των εργαζομένων που διεξάγονται μέσω πληροφοριακών συστημάτων¹¹⁸. Εάν ο εργαζόμενος ως δικαιούχος διάθεσης συναινέσει στο να λάβει ο εργοδότης γνώση των δεδομένων, τότε αποκλείεται η πλήρωση της αντικειμενικής υπόστασης του εγκλήματος, υπό την αυτονόητη βέβαια προϋπόθεση ότι η συγκατάθεση συγκεντρώνει τα στοιχεία που αναλύθηκαν πιο πάνω¹¹⁹.

Αντιθέτως, σε περίπτωση που κάποιος εργαζόμενος προβαίνει σε μη εξουσιοδοτημένη ιδιωτική χρήση των ηλεκτρονικών μέσων μιας εταιρείας και αποθηκεύει ιδιωτικά αρχεία σ' αυτά, παρά την έλλειψη σχετικής άδειας από τον εργοδότη, διατυπώνονται διάφορες απόψεις ως προς το αν τα δεδομένα αυτά εξακολουθούν να εμπίπτουν στο προστατευτικό πεδίο των παραπάνω διατάξεων. Κατά την ερμηνευτική προσέγγιση των αντίστοιχων διατάξεων του Γερμανικού Ποινικού Κώδικα, που έχουν πανομοιότυπο περιεχόμενο με τις ελληνικές, κρατούσα είναι η άποψη¹²⁰ ότι και στην περίπτωση αυτή ο εργαζόμενος πρέπει να θεωρείται ως το μόνο

¹¹⁵ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 483.

¹¹⁶ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 485· Wilkens, Internal Investigations, σελ. 527· Scharnberg, Illegale Internal Investigations, σελ. 227· Schuster, ZIS 2010, σελ. 70· Weißgerber, NZA 2003, σελ. 1008.

¹¹⁷ Wilkens, Internal Investigations, σελ. 527· Eisele σε Schönke/Schröder, StGB, § 202a πλαγ. 9· Graf σε MüKo StGB, § 202a πλαγ. 19· Hilgendorf σε LK StGB, § 202a πλαγ. 26· Kargl σε NK StGB, § 202a πλαγ. 7· Schuster σε Knierim/Rübenstahl/Tsambikakis, Internal Investigations, σελ. 318 πλαγ.129· Scharnberg, Illegale Internal Investigations, σελ. 227.

¹¹⁸ Φιλόπουλος, ο.π., ΠοινΔνη 2021, σελ. 485.

¹¹⁹ Βλ. παραπάνω σελ. 16-18.

¹²⁰ Wilkens, Internal Investigations, σελ. 528· Eisele σε Schönke/Schröder, StGB, § 202a πλαγ. 9· Schuster σε Knierim/Rübenstahl/Tsambikakis, Internal Investigations, σελ. 318 πλαγ. 130· Wolff σε LK StGB, § 303a πλαγ. 13· Eisele, Computer- und Medienstrafrecht, Κεφ. 4 πλαγ. 13· Reeb, Internal Investigations, σελ. 83· Scharnberg, Illegale Internal Investigations, σελ. 227· Eisele, ZIS 2012, σελ. 405· Hilgendorf, JuS 1996, σελ. 893· Hoeren, MMR 2013, σελ. 487επ· Schuster, ZIS 2010, σελ. 70· Weißgerber, NZA 2003, σελ. 1008.

πρόσωπο, το οποίο δικαιούται να διαθέτει αυτά τα δεδομένα, καθώς η συμπεριφορά του, παρόλο που έρχεται σε αντίθεση με τις οδηγίες του εργοδότη του, δεν επηρεάζει την πατρότητα των δεδομένων, στην οποία βασίζεται η εξουσία διάθεσης. Ωστόσο υποστηρίζεται σθεναρά και η άποψη¹²¹ ότι τα ηλεκτρονικά δεδομένα που αποθηκεύτηκαν λάθρα στα ηλεκτρονικά συστήματα της εταιρείας, παρά τις σαφείς περί του αντιθέτου οδηγίες του εργοδότη, δεν μπορούν να αποτελέσουν αντικείμενο προστασίας βάσει των ανωτέρω ρυθμίσεων, διότι αυτό θα σήμαινε ότι ο εργοδότης ως κάτοχος της μονάδας μνήμης, όπου έχουν αποθηκευτεί τα δεδομένα, δεν θα ήταν πλέον σε θέση να διαχειρίζεται τα ηλεκτρονικά συστήματα της εταιρείας στερούμενος, κατ' αυτόν τον τρόπο, ιδιοκτησιακά δικαιώματα.

Προσωπικά δεδομένα που καλύπτονται από το απόρρητο συνιστούν την αυστηρότερη κατηγορία απαγόρευσης επεξεργασίας προσωπικών δεδομένων. Ο αποχαρακτηρισμός από το απόρρητο οδηγεί την ένταξη της προστασίας των προσωπικών δεδομένων στις γενικές διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων και των συναφών εθνικών νομοθετημάτων¹²². Όπως για την ποινική ευθύνη βάσει των παραπάνω διατάξεων του Ποινικού Κώδικα που προστατεύουν το απόρρητο των επικοινωνιών, έτσι και στην περίπτωση του άρθρου 38 Ν.4624/2019 γίνεται δεκτό ότι για τη στοιχειοθέτηση της ειδικής υπόστασης των προβλεπόμενων σ' αυτό αδικημάτων σε βάρος του εργοδότη, αποφασιστικό κριτήριο είναι το εάν επιτρέπεται στον εργαζόμενο να αποθηκεύει προσωπικά αρχεία στους φορείς δεδομένων της εταιρείας ή όχι. Εάν η χρήση του υπολογιστή της εταιρείας δεν επιτρέπεται ρητά για καθαρά ιδιωτικούς σκοπούς, οι πληροφορίες που είναι αποθηκευμένες σ' αυτόν, δεν ανήκουν στην ιδιωτική σφαίρα του εργαζομένου και επομένως δεν μπορούν να είναι άξιες προστασίας¹²³. Ακόμη κι αν τα αρχεία επισημαίνονται ως «ιδιωτικά» σε περίπτωση απαγορευμένης ιδιωτικής χρήσης, η προβολή τους εξακολουθεί να χαρακτηρίζεται ως επιτρεπτή, εάν το ενδιαφέρον του εργοδότη για διευκρίνιση

¹²¹ Wilkens, Internal Investigations, σελ. 527· Beckschulze, DB 2003, σελ. 2783· Welp, iur 1988, σελ. 448· πρβλ. επίσης: Culmsee/Dorschel, CR 2013, σελ. 292;

¹²² Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το γενικό κανονισμό προστασίας δεδομένων, σελ. 124.

¹²³ ArbG Frankfurt a.M. MMR 2004, 829, 830; αυτό ισχύει ακόμα και για τις πληροφορίες που από τη φύση τους κατατάσσονται στα ευαίσθητα δεδομένα προσωπικού χαρακτήρα (πορνογραφικό υλικό), ArbG Frankfurt a.M. NZA 2002, 1093, 1095επ.· ArbG Hannover NZA 2001, 1022, 1024· βλ. επίσης: Mengel, BB 2004, σελ. 2019 m. w. Nachw.· ομοίως: Jofer/Wegerich, K&R 2002, σελ. 238· Kratz/Gubbels, NZA 2009, σελ. 654.

βασίζεται σε συγκεκριμένη υποψία για τέλεση σημαντικής παράβασης ή ποινικού αδικήματος που σχετίζεται με εργασιακή σχέση¹²⁴.

Εάν, αντιθέτως, ο εργαζόμενος είχε τη δυνατότητα χρήσης μιας μονάδας δίσκου ή φακέλου για να αποθηκεύει ιδιωτικά δεδομένα του, δικαίως πιστεύει ότι πρόκειται για προσωπικό ελεύθερο χώρο στον οποίο δεν μπορεί να έχει πρόσβαση ο εργοδότης¹²⁵. Σε αυτές τις περιπτώσεις, η επισκόπηση των εν λόγω δεδομένων αποτελεί σημαντική καταπάτηση των προσωπικών δικαιωμάτων του. Η απουσία ή η πραγματική εμπλοκή του υπευθύνου προστασίας δεδομένων και/ή του συμβουλίου εργαζομένων μπορεί επίσης να έχει ως αποτέλεσμα την επίταση ή αντίστοιχα τον μετριασμό της εν λόγω καταπάτησης¹²⁶. Το ίδιο ισχύει για τη μυστικότητα ή τη διαφάνεια του μέτρου¹²⁷.

Τέλος, σύμφωνα με την κρατούσα άποψη στη γερμανική θεωρία¹²⁸ στις περιπτώσεις που ο εργοδότης συναινεί, είτε ρητώς είτε σιωπηρώς, στη χρήση από τους εργαζόμενους των ηλεκτρονικών μέσων επικοινωνίας της επιχείρησής για ιδιωτικούς σκοπούς, επέχει θέση παρόχου τηλεπικοινωνιακών υπηρεσιών και βαρύνεται με όλες τις συναφείς υποχρεώσεις που απορρέουν από το γερμανικό νόμο περί

¹²⁴ Grützner σε Momsen/Grützner, Wirtschaftsstrafrecht, Κεφ. 4 πλαγ. 252· Salvenmoser/Schreier σε Achenbach/Ransiek, Hdb. Wirtschaftsstrafrecht, σελ. 1698 πλαγ.111· Herrmann/Soiné, NJW 2011, σελ. 2927επ· Mengel, BB 2004, σελ. 2019· ομοίως Mengel/Ullrich, NZA 2006, σελ. 241· Wisskirchen/Glaser, DB 2011, σελ. 1450.

¹²⁵ LAG Hamm BeckRS 2004, 30460285· LAG Köln NZA-RR 2004, 527, 528. Πρβλ. επίσης Schürtle/Olbers, CCZ 2010, σελ. 181.

¹²⁶ LAG Rheinland-Pfalz BeckRS 2015, 68577· LAG Berlin-Brandenburg NZA-RR 2011, 342, 345· Fülbier/Splittgerber, NJW 2012, σελ. 2000.

¹²⁷ BAG NZA 2014, 143· LAG Berlin-Brandenburg BeckRS 2016, 67048· πρβλ. επίσης LAG Berlin-Brandenburg BeckRS 2016, 67048.

¹²⁸ Ενδεικτικά βλ. OLG Karlsruhe CR 2005, 288, 289· LAG Hessen NZA-RR 2019, 130, 132· ArbG Hannover NZA-RR 2005, 420, 421· Altenhain σε MüKo StGB, § 206 πλαγ.17· Altvater σε LK StGB, §206 πλαγ.12· Eckhardt σε Spindler/Schuster, Recht der elektronischen Medien, TKG, § 88 πλαγ. 27· Heun, Hdb. TK- Recht, Teil L πλαγ. 76· Fetzer σε Arndt/Fetzer/Scherer/Graulich, TKG, § 3 πλαγ. 27· Hegewald σε MüAnwHdb IT-R, Teil 8 πλαγ. 82· v. Hehn/Hartung σε Wieland/Steinmeyer/Grüniger, Hdb. Compliance-Management, σελ. 598· Kargl σε NK StGB, § 206 πλαγ. 10· Kreitner σε Küttner, Personalbuch 2020, Internet-/Telefon- Nutzung πλαγ. 7· Meister/Laun in Wissmann, Telekommunikationsrecht, Κεφ. 14 πλαγ. 11· Munz σε Taeger/Gabel, BDSG, § 88 TKG πλαγ. 20· Panzer-Heemeier σε Grobys/Panzer-Heemeier, StichwortKommentar Arbeitsrecht, Mitarbeiterkontrolle πλαγ. 5· Polenz σε Taeger/Pohle, Computerrechts-Hdb., Teil 13, Telekommunikation und Telemedien πλαγ. 25· Ruhmannseder σε Schulz/Reinhart/ Sahan, FS I. Roxin, σελ. 512· Salvenmoser/Schreier σε Achenbach/Ransiek, Hdb. Wirtschaftsstrafrecht, σελ. 1700 πλαγ. 118· BITKOM, Die Nutzung von E-Mail und Internet im Unternehmen, σελ.19· Däubler, Gläserne Belegschaften?, πλαγ. 338· Elschner, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, σελ. 164επ· Heinson, IT-Forensik, σελ. 314· Kirsch, Datenschutz im Unternehmen, σελ. 109επ· Lackner/Kühl, StGB, § 206 πλαγ. 2· Neumann, Zur Anwendbarkeit des Fernmeldegeheimnisses, σελ. 37· Reeb, Internal Investigations, σελ. 88· v. Rosen, Internal Investigations, σελ. 83.

τηλεπικοινωνιών¹²⁹. Μέρος των ως άνω υποχρεώσεων αναφέρονται και στην προστασία των προσωπικών δεδομένων των χρηστών των τηλεπικοινωνιακών υπηρεσιών, που στην προκειμένη περίπτωση είναι οι εργαζόμενοι της επιχείρησης, οι οποίοι λογίζονται ως τρίτοι κατά την έννοια της παραγράφου 3αρ.10 του γερμανικού νόμου περί τηλεπικοινωνιών κι έχουν αξίωση στην ιδιωτική χρήση του τηλεφώνου, του ηλεκτρονικού ταχυδρομείου και του διαδικτύου κατά παραχώρηση του εργοδότη¹³⁰. Η άποψη αυτή, ωστόσο, δεν γίνεται δεκτή ούτε από τη γερμανική¹³¹ ούτε από την ελληνική νομολογία. Σχετικά ο Άρειος Πάγος συνεδριάζοντας σε Ολομέλεια εξέδωσε την υπ' αριθμόν 1/2017 απόφασή του¹³², με την οποία δέχτηκε ότι ο Ν.3471/2006 δεν βρίσκει εφαρμογή στην προκειμένη περίπτωση, γιατί ο εργοδότης δεν έχει έναντι των εργαζομένων την ιδιότητα του «παρόχου διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών» κατά την έννοια του άρθρου 3 του ίδιου νόμου. Σε επίπεδο ελληνικού δικαίου, η άποψη αυτή κρίνεται ως ορθότερη ενόψει της στενής εννοιολογικής προσέγγισης του όρου «υπηρεσίες ηλεκτρονικών επικοινωνιών» στο άρθρο 2 παρ.8 του Ν.3471/2006 και της σαφούς επιφύλαξης υπέρ των εκάστοτε ισχυουσών για την προστασία των προσωπικών δεδομένων διατάξεων στο άρθρο 4 του ίδιου νόμου.

¹²⁹ Αντιθέτως σε περίπτωση άρνησης του εργοδότη να επιτρέψει τη χρήση από τους εργαζόμενους των ηλεκτρονικών μέσων επικοινωνίας της επιχείρησης για ιδιωτικούς σκοπούς όπως έχει δικαίωμα να πράξει, δεν έχουν εφαρμογή οι ρυθμίσεις του νόμου περί των τηλεπικοινωνιών και δε γεννάται μεταξύ του εργοδότη και του εργαζομένου σχέση παρόχου-χρήστη.

¹³⁰ Baumgartner: Telefon-, Internet- und E-mail-Nutzung, einschließlich Privatnutzung (mit Betriebsvereinbarungsvorschlag) σε: Daten- und Persönlichkeitsschutz im Arbeitsverhältnis - Praxishandbuch zum Arbeitnehmerdatenschutz, hrsg. von Stephan Weth, Maximilian Herberger und Michael Wächter, σελ. 378-380.

¹³¹ LAG Berlin-Brandenburg BeckRS 2016, 67048· NZA-RR 2011, 342, 343· LAG Niedersachsen MMR 2010, 639, 640· VGH Mannheim NVwZ-RR 2015, 161, 165· ArbG Berlin BeckRS 2011, 70280· VG Karlsruhe NVwZ-RR 2013, 797, 801· Graulich σε Arndt/Fetzer/Scherer/Graulich, TKG, § 88 πλαγ. 81· Thüsing σε Thüsing, Beschäftigtendatenschutz und Compliance, §3 πλαγ.74επ.· Traut σε Thüsing/Wurth, Social Media im Betrieb, σελ. 169 πλαγ. 12· Scharnberg, Illegale Internal Investigations, σελ.113· Wittek, Soziale Netzwerke im Arbeitsrecht, σελ. 214επ.· Wybitul/Schultze-Melling, Datenschutz im Unternehmen, σελ.110 πλαγ. 273· Barton, CR 2003, σελ. 843· Behling, CB 2013, σελ. 265επ.· Buschbaum/Rosak, DB 2014, σελ. 2530επ.· Deiters, ZD 2012, σελ.110επ.· Diercks, K&R 2014, σελ.5επ.· Fülbiel/Splittgerber, NJW 2012, σελ. 1999· Haußmann/Krets, NZA 2005, σελ. 260· Jousen, NZA-Beil. 1/2011, σελ. 39· Löwisch, DB 2009, σελ. 2782επ.· Mückenberger/Müller, BB 2011, σελ. 2302επ.· Rübenthal/Debus, NZWiSt 2012, σελ.133· Scheben/Klos, CCZ 2013, σελ.89επ.· Schuster, CR 2014, σελ. 21· Seffer/Schneider, ITRB 2007, σελ. 266· Walther/Zimmer, BB 2013, σελ. 2933επ.· Wybitul, NJW 2014, σελ. 3607.

¹³² ΤΝΠ ΝΟΜΟΣ.

V. Ποινική ευθύνη εργαζομένου κατά τη χρήση των ηλεκτρονικών μέσων επικοινωνίας

Η πολυεπίπεδη προστασία που, κατά τα ανωτέρω, παρέχεται μέσω των διεθνών και εθνικών νομοθετημάτων στους εργαζομένους κατά τη χρήση των ηλεκτρονικών μέσων επικοινωνίας μιας επιχείρησης, επ' ουδενί σημαίνει ότι κατά την εν λόγω χρήση αυτοί μπορούν να παραβιάζουν το νόμο ή να προβαίνουν σε πράξεις που στρέφονται κατά του συμφέροντος της επιχείρησης ή ενδεχομένως να θίγουν δικαιώματα πνευματικής ιδιοκτησίας. Προστασία προσωπικών δεδομένων δεν σημαίνει απόλυτη απαγόρευση συλλογής κι επεξεργασίας στοιχείων που αφορούν ένα πρόσωπο και αυτό ισχύει και στην περίπτωση του εργαζόμενου. Το δικαίωμα προστασίας των προσωπικών δεδομένων υπόκειται σε περιορισμούς, οι οποίοι δικαιολογούνται από την ανάγκη προστασίας του δημοσίου συμφέροντος ή συμφερόντων άλλων προσώπων. Και από την πλευρά του εργοδότη συντρέχουν άξια προστασίας συμφέροντα, επίσης συνταγματικά κατοχυρωμένα (άρθρ. 5παρ.1, 5Α Συντ.), τα οποία επιβάλλουν τη συλλογή και επεξεργασία στοιχείων που αφορούν το πρόσωπο του εργαζομένου κατά τη διάρκεια λειτουργίας της εργασιακής σχέσης .

Παράλληλα, η κοινωνία έχει το χρέος να θέτει κανόνες, τους οποίους οφείλει να σέβεται ο εργαζόμενος ως χρήστης τηλεπικοινωνιακών υπηρεσιών και να αντιλαμβάνεται πως η μεταφορά στον πραγματικό κόσμο της εικονικής πραγματικότητας που προσφέρεται μέσω του διαδικτύου, συνεπάγεται ευθύνες. Σε περίπτωση δε που υπάρχουν βάσιμες υποψίες ότι ο εργαζόμενος, κάνοντας χρήση των ηλεκτρονικών μέσων επικοινωνίας μιας επιχείρησης, γνωστοποιεί σε τρίτους επιχειρηματικά απόρρητα ή διαπράττει άλλες ποινικά κολάσιμες πράξεις (π.χ διατύπωση ρατσιστικών ή εξυβριστικών σχολίων, δόλια επέμβαση – «σαμποτάζ» στα ηλεκτρονικά συστήματα της επιχείρησης, αθέμιτη διάδοση επιχειρηματικών απορρήτων και άλλων εταιρικών στοιχείων - πληροφοριών, επίσκεψη σε ιστοσελίδες πορνογραφικού περιεχομένου, κατασκοπεία), τότε ο εργοδότης νομιμοποιείται να προβεί σε έλεγχο της ηλεκτρονικής επικοινωνίας του εργαζομένου. Ακόμα κι αν έχει επιτραπεί απεριόριστα η προσωπική χρήση των μέσων επικοινωνίας μιας επιχείρησης, δεν επιτρέπονται παραβιάσεις του νόμου ή πράξεις που στρέφονται κατά του συμφέροντος της επιχείρησης. Επίσης, δεν επιτρέπονται πράξεις που θίγουν

δικαιώματα πνευματικής ιδιοκτησίας ή το δικαίωμα της προσωπικότητας (filesharing) έστω κι αν δεν υπάρχει ρητή απαγόρευση¹³³.

Και στην περίπτωση όμως αυτή, ο έλεγχος επιτρέπεται για περιορισμένο χρονικό διάστημα, δηλαδή μέχρις ότου επιβεβαιωθούν οι υποψίες ή αποδειχθεί, μετά πάροδο ορισμένου χρονικού διαστήματος, ότι ο έλεγχος αυτός ουδέν προσφέρει στην αποκάλυψη των παραβάσεων από την πλευρά του εργαζομένου. Σε περίπτωση που εξακριβωθεί η τέλεση αξιόποινων ή παραβατικών πράξεων από τον εργαζόμενο, ο εργοδότης μπορεί να προβεί σε προειδοποίηση και, σε περίπτωση μη συμμόρφωσης, σε καταγγελία της σύμβασης εργασίας. Παράλληλα, μπορεί να ενημερώσει τις εισαγγελικές αρχές, προσκομίζοντας όλα τα σχετικά έγγραφα και καταθέτοντας ως μάρτυρας, εκτός κι αν κωλύεται λόγω ιδιότητας (λχ. δικηγόρος) σύμφωνα με το άρθρο 212 ΚΠΔ.

Σε επίπεδο νομολογίας χαρακτηριστική είναι η απόφαση του ΕΔΔΑ στην υπόθεση Libert κατά Γαλλίας¹³⁴. Η υπόθεση αυτή αφορούσε την απόλυση υπαλλήλου της SNCF (γαλλικής εθνικής σιδηροδρομικής εταιρείας), αφοτου η κατάσχεση του υπολογιστή εργασίας του αποκάλυψε την αποθήκευση αρχείων πορνογραφικού περιεχομένου και πλαστών πιστοποιητικών που είχαν συνταχθεί για τρίτους. Ο προσφεύγων κατήγγειλε ειδικότερα ότι ο εργοδότης του είχε ανοίξει, εν τη απουσία του, προσωπικά αρχεία αποθηκευμένα στον σκληρό δίσκο του υπολογιστή εργασίας του. Το Δικαστήριο έκρινε ότι δεν υπήρξε παραβίαση του άρθρου 8 της Σύμβασης, κρίνοντας ότι στην προκειμένη περίπτωση οι γαλλικές αρχές δεν είχαν υπερβεί το περιθώριο αξιολόγησης που είχαν στη διάθεσή τους (σκ. 53). Το Δικαστήριο σημείωσε ειδικότερα ότι η αναζήτηση των αρχείων του προσφεύγοντος από τον εργοδότη είχε ως νόμιμο στόχο την προστασία των δικαιωμάτων του εργοδότη, ο οποίος δικαιολογημένα επιθυμούσε, να διασφαλίσει ότι οι υπάλληλοί του χρησιμοποιούσαν τις ηλεκτρονικές εγκαταστάσεις που είχε θέσει στη διάθεσή τους σύμφωνα με τις συμβατικές τους υποχρεώσεις και τους ισχύοντες κανονισμούς (σκ. 46).

¹³³ Baumgartner, Telefon-, Internet- und E-mail-Nutzung, einschließlich Privatnutzung (mit Betriebsvereinbarungs-vorschlag im Praxishandbuch zum Arbeitnehmerdatenschutz, σελ. 370.

¹³⁴ Διαθέσιμη σε <https://hudoc.echr.coe.int>.

Συμπερασματικές σκέψεις

Ανεξαρτήτως της γραμμής που ο εκάστοτε εργοδότης τηρεί ως προς το δικαίωμα χρήσης από τους εργαζομένους των ηλεκτρονικών μέσων επικοινωνίας της επιχείρησης (για υπηρεσιακούς σκοπούς αποκλειστικά ή όχι), ουδόλως υποχωρεί η υποχρέωσή του για προστασία της προσωπικότητας του εργαζόμενου, η οποία μεταξύ άλλων περιλαμβάνει και την προστασία των προσωπικών δεδομένων του. Με τις ραγδαίες εξελίξεις της τεχνολογίας και τους μεγάλους κινδύνους που προκύπτουν για την ιδιωτική σφαίρα του ατόμου, η προστασία προσωπικών δεδομένων, ιδίως στο χώρο των εργασιακών σχέσεων, έχει ιδιαίτερη σημασία.

Ωστόσο, λόγοι που συνέχονται με την επιχειρηματική ελευθερία του εργοδότη και την διαφύλαξη των δικών του δικαιωμάτων, επιβάλλουν τη διενέργεια εσωτερικών ερευνών, με απώτερο σκοπό τον εντοπισμό τυχόν εγκληματικών ή εν γένει παραβατικών συμπεριφορών των εργαζομένων. Μεταξύ των διερευνητικών μέτρων που επιστρατεύονται είναι και η επεξεργασία ηλεκτρονικών δεδομένων των εργαζομένων, τα οποία, πέραν του προσωπικού χαρακτήρα τους, ενίοτε εμπίπτουν και στο προστατευτικό πεδίο του τηλεπικοινωνιακού απορρήτου. Κατά την εν λόγω επεξεργασία πρέπει να τηρούνται απαρέγκλιτα οι όροι και οι αρχές που ισχύουν για την προστασία των προσωπικών δεδομένων, με βάση τον Κανονισμό για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (Γ.Κ.Π.Δ.) και το Ν. 4624/2019 και υπό το φως των επιταγών της ΕΣΔΑ και του ΧΘΔΕΕ. Σε περίπτωση μη συμμόρφωσης του εργοδότη με τις εν λόγω επιταγές, γεννιούνται στο πρόσωπό τους σοβαρές ποινικές ευθύνες για παραβίαση του τηλεπικοινωνιακού απορρήτου και των προσωπικών δεδομένων. Ποινικές ευθύνες μπορούν ωστόσο να γεννηθούν και στο πρόσωπο του εργαζόμενου, ιδίως όταν, παραγνωρίζοντας όρους που έχουν τεθεί από τον εργοδότη για τη χρήση των ηλεκτρονικών μέσων μιας εταιρείας, υποπίπτει σε συμπεριφορές, οι οποίες ενέχουν ποινικά στοιχεία και μπορούν να θέσουν σε κίνδυνο την οικονομική και νομική υπόσταση της επιχείρησης.

Βιβλιογραφία

1. Αλεξανδροπούλου-Αιγυπτιάδου, Β. (2016): Προσωπικά Δεδομένα.
2. Αναγνωστόπουλος, Η.: Σχολιασμός επί του υπ' αριθμόν 1317/2001 βουλεύματος του Αρείου Πάγου, ΠοινΧρ 2002, 435.
3. Αναστασόπουλος, Δ. (2016): Η ποινική προστασία προσωπικών δεδομένων σε Α. Κοτσαλή. Προσωπικά Δεδομένα 2016.
4. Δημητρόπουλος, Α. (2008): Συνταγματικά Δικαιώματα, 2^η εκδ.
5. Δούκα, Β. (2011): Η προστασία των προσωπικών δεδομένων στη σχέση εργασίας.
6. Δούκα, Β. : Προσωπικά δεδομένα και εργασιακές σχέσεις. Προστασία σύμφωνα με το Γενικό Κανονισμό Προστασίας Δεδομένων. ΕΕργΔ 2018, 641.
7. Ζερδελής, Δ. (2019): Εργατικό Δίκαιο - Ατομικές Εργασιακές Σχέσεις , 4η εκδ.
8. Θεοδόσης Γ., Βασικές αρχές προστασίας των προσωπικών δεδομένων των εργαζομένων, ΔΕΕ 2006, 592.
9. Ιγγλεζάκης, Ι. (2018): Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) - Το νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων.
10. Ιγγλεζάκης, Ι. (2018): Δίκαιο Πληροφορικής, 3η έκδ.
11. Κουκιάδης Δ. (2019): Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το Γενικό Κανονισμό Προστασίας Δεδομένων.
12. Κουκιάδης Ι. (2021): Εργατικό Δίκαιο - Ατομικές εργασιακές σχέσεις και το δίκαιο της ευελιξίας της εργασίας, 9η έκδ.
13. Λαδάς, Δ. (2018): Το δικαίωμα της προσωπικότητας του εργαζομένου.
14. Λεμπέσης Δ.: Γενικός Ευρωπαϊκός Κανονισμός για την προστασία προσωπικών δεδομένων (ΕΕ 2016/679) – Κατάργηση της Οδηγίας 95/46/ΕΚ – Συγκριτική μελέτη, ΔΕΝ 497 επ.
15. Μαλαγαρδή, Α. (2010): Νέες Τεχνολογίες - Προσωπικά Δεδομένα και Εργατικό Δίκαιο.
16. Μαλαγαρδή. Α. : Υπηρεσίες κοινωνικής δικτύωσης και εργασιακές σχέσεις, ΕεργΔ 2014, 232.
17. Μαργαρίτης Λ. /Σατλάνης Κ. /Φαρσεδάκης Ι.: Διάλογος με την πρόσφατη Ποινική Νομολογία ΜΕΡΟΣ Α΄, ΠοινΔικ 2016, 1 επ.

18. Μήτρου, Λ. (2016): Η προστασία δεδομένων των εργαζομένων σε Λ.Κοτσαλή, Προσωπικά Δεδομένα 2016.
19. Μήτρου, Λ. (2017): Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων - Νέο Δίκαιο - Νέες Υποχρεώσεις - Νέα Δικαιώματα.
20. Μήτρου, Λ.: Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις, ΕεργΔ 2014, 232.
21. Παναγοπούλου-Κουτνατζή Φ. (2017): Ο Γενικός Κανονισμός για την προστασία δεδομένων 679/2016/ΕΕ.
22. Παπαϊωάννου Αθ., Ο έλεγχος από τον εργοδότη της ηλεκτρονικής αλληλογραφίας και της ενασχόλησης του μισθωτού με το διαδίκτυο, ΕΕργΔ 2006, σελ. 729.
23. Σαχκεκίδου/Ταγαρά (2020): Κατ' άρθρον ερμηνεία του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ.
24. Σκουρής, Β. (2020): Συνθήκη της Λισσαβώνας, ερμηνεία κατ' άρθρον.
25. Φιλόπουλος Π., Η ποινική προστασία των τηλεπικοινωνιών – Μια πρώτη ερμηνευτική προσέγγιση των βασικών διατάξεων, ΠοινΔνη 2021, σελ. 473.
26. Χριστοδούλου, Κ. (2016): Η απόφαση του ΔΕΕ για την ακύρωση της Οδηγίας 2006/24 για την διατήρηση δεδομένων των ηλεκτρονικών επικοινωνιών σε Τιμητικό Τόμο Νικολάου Κ. Κλαμαρή.
27. Achenbach, H./ Ransiek, A. (2015): Handbuch Wirtschaftsstrafrecht.
28. Arndt, Hans-Wolfgang / Fetzer, T. / Scherer, J./ Graulich, K. (2015), TKG, 2η έκδ.
29. Barton, Dirk-M.: Betriebliche Übung und private Nutzung des Internetarbeitsplat- zes, Neue Zeitschrift für Arbeitsrecht (NZA) 2006, σελ. 460 - 466.
30. Baumgartner, U. (2014): Telefon-, Internet- und E-mail-Nutzung, einschließlich Privatnutzung (mit Betriebsvereinbarungsvorschlag) in: Daten Und Persönlichkeitsschutz im Arbeitsverhältnis- Praxishandbuch - Arbeitnehmerdatenschutz hrsg. von Stephan Weth, Maximilian Herberger und Michael Wächter, 2014.
31. Behling, Thorsten B.: Der Zugriff auf dienstliche E-Mail-Postfächer im Lichte der aktuellen Rechtsprechung, Compliance-Berater (CB) 2013, σελ. 265 - 269.
32. Beckschulze, M.: Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz, Der Be- trieb (DB) 2003, σελ. 2777 - 2786.

33. Benz, J. / Klindt, T. (2010): Compliance 2020 - ein Blick in die Zukunft, Betriebs- Berater (BB).
34. Brexl, T., Compliance: Viele Fragen ungeklärt, Anwaltsblatt (AnwBl) 2010, σελ. 498.
35. Brink, S.: Die private E-Mail-Nutzung am Arbeitsplatz, ArbR 5/2018, s. 111-136.
36. Brunhöber, B.: Privatisierung des Ermittlungsverfahrens im Strafprozess, Golt-dammers Archiv für Strafrecht (GA) 2010, σελ. 571 - 588.
37. Bürkle, J. / Hauschka, C. (2015): Der Compliance Officer.
38. Buschbaum, J. / Rosak, P.: Der Zugriff des Arbeitgebers auf den E-Mail-Account des Arbeitnehmers, Der Betrieb (DB) 2014, σελ. 2530 - 2533.
39. Byers, P: Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, NZA 2017, 1086.
40. Culmsee, T. / Dorschel, J.: E-Mails als Nebenpflicht – Treuepflichten bei der Bereitstellung von E-Mail-Accounts, Computer und Recht (CR) 2013, σελ. 290 - 294.
41. Däubler, W.: Informationsbedarf versus Persönlichkeitsschutz - was muss, was darf der Arbeitgeber wissen?, NZA 23/2017, s. 1481 επ.
42. Däubler, W. (2015): Gläserne Belegschaften?, 6η έκδ.
43. Däubler, W. (2015): Internet und Arbeitsrecht, Web 2.0, Social Media und Crowdwork.
44. Deiters, G.: Betriebsvereinbarung Kommunikation, Zeitschrift für Datenschutz (ZD) 2012, σελ. 109 - 115.
45. Diercks, N.: Social Media im Unternehmen, Kommunikation & Recht (K&R) 2014, σελ. 1 - 7.
46. Eisele, J. (2012): Compliance und Datenschutzstrafrecht.
47. Eisele, J. (2013): Computer- und Medienstrafrecht.
48. Eisele, J.: Arbeitnehmerüberwachung und Compliance unter Berücksichtigung der Cybercrime-Konvention, Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2012, σελ. 402 - 408.
49. Elschner, G. (2004): Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz.
50. Fischer, T. (2016): Strafgesetzbuch mit Nebengesetzen.

51. Fuhrmann, L.: Internal Investigations: Was dürfen und müssen die Organe beim Verdacht von Compliance Verstößen tun?, Neue Zeitschrift für Gesellschaftsrecht (NZG) 2016, σελ. 881 - 889.
52. Fülbier, U. / Splittgerber, A.: Keine (Fernmelde-)Geheimnisse vor dem Arbeitgeber?, Neue Juristische Wochenschrift (NJW) 2012, σελ. 1995 - 2001.
53. Golombek, T.: Pflichten von Geschäftsleitungs- und Überwachungsorganen bei Verdacht auf Unregelmäßigkeiten im Unternehmen, Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V. (WiJ) 2012, σελ. 162 - 170.
54. Greeve, G.: Privatisierung behördlicher Ermittlungen, Strafverteidiger Forum (StraFo) 2013, σελ. 89 – 96.
55. Grobys, M. / Panzer-Heemeier, A. (2016), StichwortKommentar Arbeitsrecht, 2η έκδ.
56. Haußmann, K. / Krets, J., EDV-Betriebsvereinbarungen im Praxistest, Neue Zeitschrift für Arbeitsrecht (NZA) 2005, σελ. 259 - 264.
57. Heinson, D. (2015): IT-Forensik.
58. Herrmann, K. / Soiné, M.: Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, Neue Juristische Wochenschrift (NJW) 2011, σελ. 2922 - 2928.
59. Heun, Sven-Erik (2007), Handbuch Telekommunikationsrecht, 2η έκδ.
60. Heutz, S.: Zur Pflicht der Gesellschaft zur Übernahme von Rechtsverteidigungskosten im Zusammenhang mit Compliance-Verstößen ihrer Geschäftsführer, Der Betrieb (DB) 2012, σελ. 902 - 904.
61. Hilgendorf, E.: Grundfälle zum Computerstrafrecht, Juristische Schulung (JuS) 1996, σελ. 890 - 894.
62. Hoeren, T.: Dateneigentum, MultiMedia und Recht (MMR) 2013, S. 486 - 491.
63. Hoffmann, Volker H. / Wißmann, Anke C.: Die Erstattung von Geldstrafen, Geldauflagen und Verfahrenskosten im Strafverfahren durch Wirtschaftsunternehmen gegenüber ihren Mitarbeitern, Strafverteidiger (StV) 2001, σελ. 249 - 252.
64. Hölters, W. (2017): Aktiengesetz Kommentar, 3^η έκδ.
65. Hugger, H.: Unternehmensinterne Untersuchungen - Erfahrungen und Standards der Praxis, Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR) 2015, σελ. 214 - 225.
66. Inderst, C. / Bannenberg, B. / Poppe, S. (2017): Compliance, 3^η έκδ.

67. Jarass, H. (2021): Charta der Grundrechte der Europäischen Union: GRCh.
68. Jofer, R. / Wegerich, C.: Betriebliche Nutzung von E-Mail-Diensten: Kontrollbefugnisse des Arbeitgebers, Kommunikation & Recht (K&R) 2002, σελ. 235 - 240.
69. Joussem, J.: Mitarbeiterkontrolle: Was muss, was darf das Unternehmen wissen?, Neue Zeitschrift für Arbeitsrecht (NZA) τεύχος 1/2011, σελ.. 35 - 42.
70. Kahlenberg, H. / Schwinn, H.: Amnestieprogramme bei Compliance-Untersuchungen im Unternehmen, Corporate Compliance Zeitschrift (CCZ) 2012, σελ. 81 - 86.
71. Kempf, E. / Lüderssen, K. / Volk, K. (2012): Unternehmensstrafrecht.
72. Kirsch, M. (2011), Datenschutz im Unternehmen.
73. Knauer, C.: Interne Ermittlungen (Μέρος 1^ο) - Grundlagen, Zeitschrift für Wirtschaftsstrafrecht und Haftung im Unternehmen (ZWH) 2012, σελ. 41- 48.
74. Knauer, C./ Gaul, M.: Internal investigations und fair trial, Neue Zeitschrift für Strafrecht (NStZ) 2013, σελ. 192 - 194.
75. Knierim, Th. C. / Rübenstahl, M. / Tsambikakis, M. (2013): Internal Investigations: Ermittlungen im Unternehmen.
76. Kramer, S.: Folgen der EGMR Rechtsprechung für eine IT-Kontrolle bei Privatnutzungsverbot, NZA 10/2018, σελ. 637-640.
77. Kramer, S. (2014): Betriebsrat und Datenschutz in: Daten-und Persönlichkeitsschutz im Arbeitsverhältnis - Praxishandbuch zum Arbeitnehmerdatenschutz, hrsg. von Stephan Weth, Maximilian Herberger und Michael Wächter.
78. Kuhlen, L.: Zum Verhältnis von strafrechtlicher und zivilrechtlicher Haftung für Compliance-Mängel, Μέρος 1, Neue Zeitschrift für Wirtschafts- Steuer- und Unternehmensstrafrecht (NZWiSt) 2015, σελ. 121 - 129.
79. Küttner, W. (2020): Personalbuch 2020, 27η έκδ..
80. Löwisch, M., Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, Der Betrieb (DB) 2009, σελ. 2782 – 2787.
81. Mansdörfer, M.: Die Aussagepflicht der Mitarbeiter bei wertebasierten unternehmensinternen Ermittlungen, juris - Die Monatszeitschrift (JM) 2014, σελ. 167 – 173.
82. Mengel, A.: Kontrolle der E-mail- und Internetkommunikation am Arbeitsplatz, Betriebs-Be-rater (BB) 2004, σελ. 2014 - 2021.

83. Mengel, A. / Ullrich, T.: Arbeitsrechtliche Aspekte unternehmensinterner Investigations, Neue Zeitschrift für Arbeitsrecht (NZA) 2006, σελ. 240 – 246.
84. Momsen, C. / Grützner, T. (2013): Wirtschaftsstrafrecht.
85. Mückenberger, O./Müller, Cl. A.: LAG Berlin-Brandenburg verneint Diensteanbietereigenschaft des Arbeitgebers i.S.d. TKG und damit Strafbarkeit nach §206 StGB bei Sichtung von E-Mails, Betriebs-Berater (BB) 2011, σελ. 2302 - 2303.
86. Neumann, A. (2014): Zur Anwendbarkeit des Fernmeldegeheimnisses nach § 88 TKG bei gestatteter Privatnutzung betrieblicher Telekommunikationsmöglichkeiten.
87. Pfordte, T.: σε AG StrafR-DAV, Strafverteidigung im Rechtsstaat, σελ. 740.
88. Poller, S.: Untreue durch Übernahme von Geldsanktionen, Verfahrenskosten und Verteidigerhonoraren?, Strafverteidiger Forum (StraFo) 2005, σελ. 274 - 283.
89. Reeb, P. (2011): Internal Investigations.
90. Rönna, T. / Schneider, F.: Der Compliance-Beauftragte als strafrechtlicher Garant: Überlegungen zum BGH-Urteil v. 17.7.2009 - 5 StR 394/08, ZIP 2009, 1867, Zeitschrift für Wirtschaftsrecht (ZIP) 2010, σελ. 53 - 61.
91. Rotsch, T., Criminal Compliance, Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2010, σελ. 614 - 617.
92. Rübenstahl, M. / Debus, St.: Strafbarkeit verdachtsabhängiger E-Mail- und EDV-Kontrollen bei Internal Investigations?, Neue Zeitschrift für Wirtschafts- Steuer- und Unternehmensstrafrecht (NZWiSt) 2012, σελ. 129 - 137.
93. Scharnberg, J. (2015): Illegale Internal Investigations.
94. Scheben, B. / Klos, C.: Analyse von Chatprotokollen und E-Mails - Was ist erlaubt? Was ist verwertbar?, Corporate Compliance Zeitschrift (CCZ) 2013, σελ. 88 - 93.
95. Schober, J.Q Spürhunde auf der Jagd, Focus Spezial 10-11/2017, σελ. 16 - 21.
96. Schönke, A. / Schröder, H. (2019): Strafgesetzbuch Kommentar, 30η έκδ.
97. Schott, S., Zahlung von Sanktionen und Verteidigungskosten für Mitarbeiter durch Unternehmen, Strafverteidiger Forum (StraFo) 2014, σελ. 315 - 324.
98. Schulz, L. / Reinhart, M. / Sahan, O. (2012): Festschrift für Imme Roxin.
99. Schulze-Heiming, I. (1995): Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls.

100. Schürle, T. / Olbers, Lucie Anne Mary: Praktische Hinweise zu Rechtsfragen bei eigenen Untersuchungen im Unternehmen, Corporate Compliance Zeitschrift (CCZ) 2010, σελ. 178 – 182.
101. Schuster, Fr. P.: IT-gestützte interne Ermittlungen in Unternehmen - Strafbarkeitsrisiken nach den §§ 202a, 206 StGB, Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2010, σελ. 68 – 75.
102. Schuster, F.: Der Arbeitgeber und das Telekommunikationsgesetz, Computer und Recht (CR) 2014, σελ. 21 - 27.
103. Seffer, A. / Schneider, J., Behandlung des E-Mail-Accounts ausgeschiedener Organmitglieder, IT-Rechtsberater (ITRB) 2007, σελ. 264 - 267.
104. Spatscheck, R. / Ehnert, M.: Übernahme von Geldsanktionen und Verteidigerhonorar - Straf- und steuerrechtliche Aspekte -, Strafverteidiger Forum (StraFo) 2005, σελ. 265 - 273.
105. Spindler, G. / Schuster, F. (2015): Recht der elektronischen Medien, 3η έκδ.
106. Taschke, J.: Zur Entwicklung der Verfolgung von Wirtschaftsstrafsachen in der Bundesrepublik Deutschland, Μέρος 3: Auf dem Weg zur Privatisierung der Strafverfolgung, Neue Zeitschrift für Wirtschafts- Steuer- und Unternehmensstrafrecht (NZWiSt) 2012, σελ. 89 - 94.
107. Taeger, J. / Pohle, J. (2018): Computerrechts-Handbuch.
108. Thüsing, G. / Wurth, G. (2015): Social Media im Betrieb.
109. Thüsing, G. (2021): Beschäftigten-datenschutz und Compliance, 3η έκδ.
110. von Rosen, R. (2010): Internal Investigations bei Compliance-Verstößen.
111. Wabnitz, Heinz-Bernd / Janovsky, T. (2014): Handbuch des Wirtschafts- und Steuerstrafrechts.
112. Wagner, J.: "Internal Investigations" und ihre Verankerung im Recht der AG, Corporate Compliance Zeitschrift (CCZ) 2009, σελ. 8 - 17.
113. Walther, M./Zimmer, M.: Mehr Rechtssicherheit für Compliance-Ermittlungen, Betriebs-Berater (BB) 2013, σελ. 2933 – 2937.
114. Welp, J.: Datenveränderung (§ 303a StGB) – Μέρος 1º, Informatik und Recht (iur) 1988, σελ. 443 – 449.
115. Weißgerber, M.: Das Einsehen kennwortgeschützter Privatdateien des Arbeitnehmers durch den Arbeitgeber, Neue Zeitschrift für Arbeitsrecht (NZA) 2003, σελ. 1005 - 1009.

116. Werner, R.: Die Enthftung des Vorstands: Die strafrechtliche Dimension, Corporate Compliance Zeitschrift (CCZ) 2011, σελ.. 201 - 207.
117. Wieland, J. / Steinmeyer, R. / Grüninger, S. (2010): Handbuch Compliance-Management: Konzeptionelle Grundlagen, praktische Erfolgsfaktoren, globale Herausforderungen.
118. Wilkens, R. (2020): Internal Investigations.
119. Wisskirchen, G./ Glaser, J.: Unternehmensinterne Untersuchungen (Μέρος 1^ο), Der Betrieb (DB) 2011, σελ. 1392 - 1395.
120. Wissmann, M. (2006): Telekommunikationsrecht, 2η έκδ.
121. Wittek, Wolfgang H. (2014): Soziale Netzwerke im Arbeitsrecht.
122. Wybitul, T.: Strafbarkeitsrisiken für Compliance-Verantwortliche, BetriebsBerater (BB) 2009, σελ. 2590 - 2593.
123. Wybitul, T.: E-Mail-Auswertung in der betrieblichen Praxis, Neue Juristische Wochenschrift (NJW) 2014, σελ. 3605 - 3611.
124. Wybitul, T./ Schultze-Melling, J. (2014): Datenschutz im Unternehmen, 2η έκδ.