ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

17/EL

WP 249

Γνώμη 2/2017 σχετικά με την επεξεργασία δεδομένων στην εργασία

Εκδόθηκε στις 8 Ιουνίου 2017

Η εν λόγω ομάδα εργασίας συστάθηκε δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ. Αποτελεί ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία των δεδομένων και της ιδιωτικότητας. Τα καθήκοντά της περιγράφονται στο άρθρο 30 της οδηγίας 95/46/ΕΚ και στο άρθρο 15 της οδηγίας 2002/58/ΕΚ.

Γραμματειακή υποστήριξη παρέχεται από τη Διεύθυνση Γ (Θεμελιώδη δικαιώματα και κράτος δικαίου) της Ευρωπαϊκής Επιτροπής, Γενική Διεύθυνση Δικαιοσύνης και Καταναλωτών, Β-1049 Βρυξέλλες, Βέλγιο, Γραφείο αριθ. MO59 05/35.

Δικτυακός τόπος: http://ec.europa.eu/justice/data-protection/index_en.htm

Περιεχόμενα

1 Συνοπτική παρουσίαση

Η παρούσα γνώμη συμπληρώνει τις προηγούμενες δημοσιεύσεις της ομάδας εργασίας του άρθρου 29 («ΟΕ29») με τίτλο *Γνώμη 8/2001 για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο εργασιακό πλαίσιο* (WP48)[1] και *Έγγραφο εργασίας για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας* του 2002 (WP55)[2]. Από την έκδοση των εν λόγω εγγράφων, έχουν αρχίσει να χρησιμοποιούνται νέες τεχνολογίες οι οποίες δίνουν τη δυνατότητα πιο συστηματικής επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στην εργασία, δημιουργώντας σημαντικές προκλήσεις για την προστασία της ιδιωτικότητας και των δεδομένων.

Η παρούσα γνώμη προβαίνει σε μια νέα εκτίμηση της ισορροπίας μεταξύ των έννομων συμφερόντων των εργοδοτών και της εύλογης προσδοκίας ιδιωτικότητας την οποία έχουν οι εργαζόμενοι, περιγράφοντας τους κινδύνους που προκύπτουν από τις νέες τεχνολογίες και προβαίνοντας σε αξιολόγηση αναλογικότητας διαφόρων σεναρίων στα οποία αυτές θα μπορούσαν να χρησιμοποιηθούν.

Η γνώμη, αν και εστιάζεται πρωτίστως στην οδηγία για την προστασία των δεδομένων, εξετάζει και τις επιπρόσθετες υποχρεώσεις που επιβάλλει στον εργοδότη ο γενικός κανονισμός για την προστασία των δεδομένων. Επίσης, επαναλαμβάνει τις θέσεις και τα συμπεράσματα της γνώμης 8/2001 και του εγγράφου εργασίας WP55, και συγκεκριμένα ότι κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων:

- οι εργοδότες θα πρέπει να έχουν πάντα υπόψη τις θεμελιώδεις αρχές προστασίας των δεδομένων, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται·
- το περιεχόμενο των ηλεκτρονικών επικοινωνιών που πραγματοποιούνται σε επαγγελματικές εγκαταστάσεις απολαμβάνει την ίδια προστασία ως προς τα θεμελιώδη δικαιώματα όπως και οι αναλογικές επικοινωνίες·
- η συγκατάθεση είναι εξαιρετικά απίθανο να συνιστά νομική βάση για την επεξεργασία δεδομένων στην εργασία, εκτός εάν οι εργαζόμενοι μπορούν να αρνηθούν την επεξεργασία χωρίς αρνητικές συνέπειες·
- μπορεί ενίοτε να γίνει επίκληση της εκτέλεσης σύμβασης και των εννόμων συμφερόντων, υπό τον όρο ότι η επεξεργασία είναι αυστηρά απαραίτητη για νόμιμο σκοπό και είναι σύμφωνη με τις αρχές της αναλογικότητας και της επικουρικότητας·
- οι εργαζόμενοι θα πρέπει να λαμβάνουν αποτελεσματική ενημέρωση για την παρακολούθηση που πραγματοποιείται· και
- κάθε διεθνής διαβίβαση δεδομένων των εργαζομένων θα πρέπει να πραγματοποιείται μόνο εφόσον διασφαλίζεται κατάλληλο επίπεδο προστασίας.

2. Εισαγωγή

[1] ΟΕ29, *Γνώμη 08/2001 για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο εργασιακό πλαίσιο,* WP48, 13 Σεπτεμβρίου 2001, διεύθυνση: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] ΟΕ29, *Έγγραφο εργασίας για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας,* WP55, 29 Μαΐου 2002, διεύθυνση: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_el.pdf

Η ταχεία υιοθέτηση νέων τεχνολογιών πληροφοριών στον χώρο εργασίας ως προς τις υποδομές, τις εφαρμογές και τις έξυπνες συσκευές επιτρέπει τη διενέργεια νέου είδους συστηματική και, ενδεχομένως, παρεμβατικής επεξεργασίας δεδομένων στην εργασία. Για παράδειγμα:

- οι τεχνολογίες που δίνουν τη δυνατότητα επεξεργασίας δεδομένων στην εργασία μπορούν πλέον να χρησιμοποιούνται με κόστος πολύ μικρότερο από ό,τι πριν αρκετά χρόνια, ενώ η ικανότητα των τεχνολογιών αυτών ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα έχει αυξηθεί εκθετικά·
- οι νέες μορφές επεξεργασίας, όπως εκείνες που αφορούν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο της χρήσης επιγραμμικών υπηρεσιών και/ή δεδομένα θέσης από έξυπνη συσκευή, είναι πολύ λιγότερο ορατές για τους εργαζομένους από ό,τι οι πιο παραδοσιακές μορφές, όπως οι εμφανείς κάμερες τηλεόρασης κλειστού κυκλώματος. Αυτό εγείρει ερωτήματα σχετικά με τον βαθμό στον οποίο οι εργαζόμενοι έχουν επίγνωση των εν λόγω τεχνολογιών, καθώς οι εργοδότες θα μπορούσαν να προβαίνουν παράνομα σε μια τέτοια επεξεργασία χωρίς να γνωστοποιούν προηγουμένως το γεγονός αυτό στους εργαζόμενους· και
- τα όρια μεταξύ της προσωπικής οικίας και της εργασίας γίνονται ολοένα και πιο δυσδιάκριτα. Για παράδειγμα, όταν οι εργαζόμενοι τηλεεργάζονται (π.χ. από το σπίτι) ή βρίσκονται σε επαγγελματικό ταξίδι, μπορεί να πραγματοποιείται παρακολούθηση δραστηριοτήτων εκτός του υλικού περιβάλλοντος εργασίας, η οποία ενδέχεται να περιλαμβάνει παρακολούθηση του ατόμου σε ιδιωτικό πλαίσιο.

Ως εκ τούτου, ενώ η χρήση των τεχνολογιών αυτών μπορεί να είναι χρήσιμη για τον εντοπισμό ή την πρόληψη της απώλειας πνευματικής και υλικής εταιρικής ιδιοκτησίας, για τη βελτίωση της παραγωγικότητας των εργαζομένων και την προστασία των δεδομένων για τα οποία είναι υπεύθυνος ο υπεύθυνος επεξεργασίας, δημιουργεί επίσης σημαντικές προκλήσεις όσον αφορά την ιδιωτική ζωή και την προστασία των δεδομένων. Ως εκ τούτου, είναι αναγκαία μια νέα αξιολόγηση σχετικά με την ισορροπία μεταξύ του έννομου συμφέροντος του εργοδότη να προστατέψει την επιχείρησή του και την εύλογη προσδοκία ιδιωτικότητας που έχουν τα υποκείμενα των δεδομένων: οι εργαζόμενοι.

Ενώ η παρούσα γνώμη θα εστιαστεί στις νέες τεχνολογίες των πληροφοριών αξιολογώντας εννέα διαφορετικά σενάρια που τις αφορούν, θα εξετάσει επίσης συνοπτικά τις παραδοσιακότερες μεθόδους επεξεργασίας δεδομένων στην εργασία, οι οποίες παρουσιάζουν μεγαλύτερο κίνδυνο λόγω της τεχνολογικής αλλαγής.

Χρησιμοποιώντας τον όρο «εργαζόμενος» στην παρούσα γνώμη, σκοπός της ΟΕ29 δεν είναι να περιορίσει το πεδίο του όρου αυτού μόνο σε πρόσωπα που έχουν σύμβαση εργασίας η οποία αναγνωρίζεται στο πλαίσιο της ισχύουσας εργατικής νομοθεσίας. Τις τελευταίες δεκαετίες, έχουν γίνει συχνότερα νέα επιχειρηματικά μοντέλα που εξυπηρετούνται από διαφορετικά είδη σχέσεων εργασίας, και συγκεκριμένα εργασία σε ανεξάρτητη βάση. Η παρούσα γνώμη αποσκοπεί στην κάλυψη όλων των περιπτώσεων στις οποίες υπάρχει σχέση εργασίας, ανεξάρτητα από το αν η σχέση αυτή βασίζεται σε σύμβαση εργασίας.

Έχει σημασία να αναφερθεί ότι οι εργαζόμενοι σπάνια είναι σε θέση να δώσουν, να αρνηθούν ή να ανακαλέσουν τη συγκατάθεσή τους, δεδομένης της εξάρτησης που προκύπτει από τη σχέση μεταξύ εργοδότη και εργαζόμενου. Εκτός από εξαιρετικές περιπτώσεις, οι εργοδότες θα πρέπει να βασίζονται σε άλλη νομική βάση πλην της συγκατάθεσης – όπως η ανάγκη επεξεργασίας των δεδομένων στο πλαίσιο έννομου συμφέροντός τους. Ωστόσο, το

έννομο συμφέρον αφ' εαυτού του δεν επαρκεί για να παρακαμφθούν τα δικαιώματα και οι ελευθερίες των εργαζομένων.

Ανεξάρτητα από τη νομική βάση της εν λόγω επεξεργασίας, πριν την έναρξή της θα πρέπει να διενεργείται έλεγχος αναλογικότητας, έτσι ώστε να εξετάζεται αν η επεξεργασία είναι αναγκαία για νόμιμο σκοπό, καθώς και τα μέτρα που πρέπει να ληφθούν ώστε να διασφαλίζεται ότι οι παραβιάσεις των δικαιωμάτων στην ιδιωτικότητα και στο απόρρητο των επικοινωνιών περιορίζονται στο ελάχιστο. Αυτό μπορεί να αποτελεί μέρος εκτίμησης επιπτώσεων σχετικά με την προστασία των δεδομένων (ΕΕΠΔ).

3. Νομικό πλαίσιο

Παρόλο που η ανάλυση που ακολουθεί βασίζεται κατά κύριο λόγο στο ισχύον νομικό πλαίσιο σύμφωνα με την οδηγία 95/46/ΕΚ (οδηγία για την προστασία των δεδομένων ή «ΟΔΠ»)[3], η παρούσα γνώμη θα εξετάσει επίσης και τις υποχρεώσεις στο πλαίσιο του κανονισμού 2016/679 (γενικός κανονισμός για την προστασία δεδομένων ή «ΓΚΠΔ»)[4], ο οποίος έχει ήδη αρχίσει να ισχύει και θα τεθεί σε εφαρμογή στις 25 Μαΐου 2018.

Σχετικά με τον προτεινόμενο κανονισμό για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[5], η ομάδα εργασίας καλεί τους ευρωπαίους νομοθέτες να δημιουργήσουν μια ειδική εξαίρεση για την παρεμβολή σε συσκευές που χορηγούνται σε εργαζομένους[6]. Ο προτεινόμενος κανονισμός δεν περιλαμβάνει κατάλληλη εξαίρεση από τη γενική απαγόρευση παρεμβολής και οι εργοδότες συνήθως δεν μπορούν να παράσχουν έγκυρη συγκατάθεση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα των εργαζομένων τους.

3.1 Οδηγία 95/46/ΕΚ – οδηγία για την προστασία των δεδομένων («ΟΠΔ»)

Στη γνώμη 8/2001, η ΟΕ29 επισήμανε ότι οι εργοδότες θα πρέπει να λαμβάνουν υπόψη τις θεμελιώδεις αρχές της ΟΠΔ για την προστασία των δεδομένων κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της εργασίας. Η ανάπτυξη νέων τεχνολογιών και νέων μεθόδων επεξεργασίας σε αυτό το πλαίσιο δεν έχουν μεταβάλει την κατάσταση – στην πραγματικότητα, θα μπορούσε κανείς να πει ότι οι εξελίξεις αυτές έχουν καταστήσει *σημαντικότερη* τη σχετική ανάγκη. Στο πλαίσιο αυτό, οι εργοδότες θα πρέπει:

---

[3] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και με την ελεύθερη κυκλοφορία των δεδομένων αυτών, *ΕΕ L 281 της 23.11.1995, σ. 31-50*, σύνδεσμος: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[4] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), *ΕΕ L 119 της 4.5.2016, σ. 1-88*, σύνδεσμος: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[5] Πρόταση κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ, 2017/0003 (COD), σύνδεσμος: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241

[6] Βλέπε ΟΕ29, *Γνώμη 01/2017 σχετικά με τον προτεινόμενο κανονισμό για τον κανονισμό σχετικά με την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες*, WP 247, 4 Απριλίου 2017, σελίδα 29· σύνδεσμος: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

- να εξασφαλίζουν ότι τα δεδομένα υποβάλλονται σε επεξεργασία για συγκεκριμένους και νόμιμους σκοπούς που είναι αναλογικοί και αναγκαίοι·
- να λαμβάνουν υπόψη την αρχή του περιορισμού του σκοπού, διασφαλίζοντας παράλληλα ότι τα δεδομένα είναι επαρκή και συναφή και δεν υπερβαίνουν τον νόμιμο σκοπό τους·
- να εφαρμόζουν τις αρχές της αναλογικότητας και της επικουρικότητας ανεξαρτήτως της εφαρμοστέας νομικής βάσης·
- να εφαρμόζουν διαφάνεια προς τους εργαζομένους τους ως προς τη χρήση και τους σκοπούς των τεχνολογιών παρακολούθησης·
- να επιτρέπουν στα υποκείμενα των δεδομένων να ασκούν τα δικαιώματά τους, μεταξύ των οποίων και τα δικαιώματα πρόσβασης, και, ανάλογα με την περίπτωση, η διόρθωση, η διαγραφή ή ο αποκλεισμός των δεδομένων προσωπικού χαρακτήρα·
- να διατηρούν τα δεδομένα ακριβή και όχι για χρονικό διάστημα μεγαλύτερο από ό,τι απαιτείται· και
- να λαμβάνουν όλα τα αναγκαία μέτρα για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση και να διασφαλίζουν ότι το προσωπικό έχει επαρκή γνώση των υποχρεώσεων περί προστασίας δεδομένων.

Χωρίς να επαναλαμβάνει τις προηγούμενες γνωμοδοτήσεις, η ΟΕ29 επιθυμεί να τονίσει τρεις αρχές, και συγκεκριμένα: νομική βάση, διαφάνεια και αυτοματοποιημένες αποφάσεις.

3.1.1 *ΝΟΜΙΚΗ ΒΑΣΗ (ΑΡΘΡΟ 7)*

Κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της εργασίας, πρέπει να πληρείται ένα τουλάχιστον από τα κριτήρια του άρθρου 7. Εάν το είδος των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία περιλαμβάνει ειδικές κατηγορίες (όπως αναλύονται στο άρθρο 8), η επεξεργασία απαγορεύεται εκτός εάν ισχύει εξαίρεση[7],[8]. Εάν ο εργοδότης μπορεί να επικαλεστεί μία από τις εξαιρέσεις αυτές, για να είναι η επεξεργασία θεμιτή εξακολουθεί να απαιτείται νόμιμη βάση του άρθρου 7.

Συνοπτικά, οι εργοδότες πρέπει ως εκ τούτου να λαμβάνουν υπόψη τα εξής:

- Για το μεγαλύτερο μέρος αυτής της επεξεργασίας δεδομένων στην εργασία, **η νομική βάση δεν μπορεί και δεν πρέπει να είναι η συγκατάθεση των εργαζομένων** [άρθρο 7 στοιχείο α)], λόγω της φύσης της σχέσης μεταξύ εργοδότη και εργαζόμενου·
- η επεξεργασία μπορεί να είναι απαραίτητη **για την εκτέλεση σύμβασης** [άρθρο 7 στοιχείο β)] σε περιπτώσεις στις οποίες ο εργοδότης πρέπει να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα του εργαζόμενου για την τήρηση οποιασδήποτε τέτοιας υποχρέωσης·
- είναι πολύ σύνηθες η **εργατική νομοθεσία να επιβάλλει νομικές υποχρεώσεις** [άρθρο 7 στοιχείο γ)] **οι οποίες απαιτούν την επεξεργασία δεδομένων προσωπικού**

[7] Όπως αναφέρεται στο μέρος 8 της γνώμης 08/2001· για παράδειγμα, το άρθρο 8 παράγραφος 2 στοιχείο β) προβλέπει εξαίρεση προκειμένου να εκπληρωθούν οι υποχρεώσεις και τα ειδικά δικαιώματα του υπευθύνου της επεξεργασίας στον τομέα του εργατικού δικαίου, στον βαθμό που το επιτρέπει η εθνική νομοθεσία η οποία προβλέπει επαρκείς εγγυήσεις.

[8] Θα πρέπει να σημειωθεί ότι σε ορισμένες χώρες, υπάρχουν ειδικά μέτρα που πρέπει να εφαρμόζουν οι εργοδότες για την προστασία της ιδιωτικής ζωής των εργαζομένων. Η Πορτογαλία αποτελεί ένα παράδειγμα χώρας στην οποία υπάρχουν τέτοια ειδικά μέτρα και παρόμοια μέτρα ενδέχεται να ισχύουν και σε ορισμένα άλλα κράτη μέλη. Για τους λόγους αυτούς, τα συμπεράσματα στο μέρος 5.6, καθώς και τα παραδείγματα στο μέρος 5.1 και στο μέρος 5.7.1 της παρούσας γνώμης δεν ισχύουν επομένως στην Πορτογαλία.

χαρακτήρα· στις περιπτώσεις αυτές ο εργαζόμενος πρέπει να είναι σαφώς και πλήρως ενήμερος για την επεξεργασία αυτή (εκτός αν ισχύει εξαίρεση)·

- αν ο εργοδότης επικαλείται **έννομο συμφέρον** [άρθρο 7 στοιχείο στ)], ο σκοπός της επεξεργασίας θα πρέπει να είναι νόμιμος· η επιλεγείσα μέθοδος ή ειδική τεχνολογία θα πρέπει να είναι αναγκαία, αναλογική και να εφαρμόζεται με τον κατά το δυνατόν λιγότερο παρεμβατικό τρόπο, μαζί με την παροχή στον εργοδότη της δυνατότητας να δείξει ότι **εφαρμόζονται κατάλληλα μέτρα** ώστε να διασφαλίζεται η ισορροπία με τα θεμελιώδη δικαιώματα και ελευθερίες των εργαζομένων[9]·
- η επεξεργασία θα πρέπει επίσης να συμμορφώνεται με τις **απαιτήσεις διαφάνειας** (άρθρα 10 και 11) και οι εργαζόμενοι θα πρέπει να είναι σαφώς και πλήρως ενημερωμένοι για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα τους[10], συμπεριλαμβανομένης της ύπαρξης παρακολούθησης· και
- θα πρέπει να λαμβάνονται **κατάλληλα τεχνικά και οργανωτικά μέτρα** ώστε να διασφαλίζεται η ασφάλεια της επεξεργασίας (άρθρο 17).

Τα πιο συναφή κριτήρια βάσει του άρθρου 7 παρουσιάζονται αναλυτικά παρακάτω.

- **Συγκατάθεση [άρθρο 7 στοιχείο α)]**

Σύμφωνα με την ΟΠΔ, η συγκατάθεση ορίζεται ως κάθε δήλωση βουλήσεως, ελευθέρας, ρητής και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων δέχεται να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Για να είναι έγκυρη η συγκατάθεση, πρέπει επίσης να μπορεί να είναι ανακλητή.

Η ΟΕ29 έχει τονίσει προηγουμένως στη γνώμη 8/2001 ότι όταν ένας εργοδότης πρέπει να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα των εργαζομένων του, είναι παραπλανητικό να προβαίνει στην επεξεργασία με την εξαρχής υπόθεση ότι η επεξεργασία μπορεί να νομιμοποιηθεί μέσω της συγκατάθεσης των εργαζομένων. Σε περιπτώσεις όπου ο εργοδότης υποστηρίζει ότι απαιτείται συγκατάθεση και η μη συγκατάθεση του εργαζομένου μπορεί να οδηγήσει σε πραγματική ή δυνητική σχετική βλάβη (κάτι που μπορεί να είναι ιδιαίτερα πιθανό στο πλαίσιο της εργασίας, ιδιαίτερα όταν αφορά την παρακολούθηση του εργαζομένου από τον εργοδότη σε βάθος χρόνου), τότε η συγκατάθεση δεν είναι έγκυρη, επειδή δεν δίνεται ελεύθερα. Ως εκ τούτου, για την πλειονότητα των περιπτώσεων επεξεργασίας δεδομένων των εργαζομένων, η νομική βάση της επεξεργασίας δεν μπορεί και δεν θα πρέπει να είναι η συγκατάθεση των εργαζομένων, επομένως απαιτείται διαφορετική νομική βάση.

Επιπλέον, ακόμα και σε περιπτώσεις όπου μπορεί να χρησιμοποιηθεί το επιχείρημα ότι η συγκατάθεση αποτελεί έγκυρη νομική βάση για την επεξεργασία αυτή (αν, δηλαδή, μπορεί να εξαχθεί χωρίς αμφιβολία το συμπέρασμα ότι η συγκατάθεση δίνεται ελεύθερα), πρέπει να είναι ρητή και εν πλήρει επιγνώσει δήλωση βουλήσεως του εργαζομένου. Προεπιλεγμένες ρυθμίσεις σε συσκευές και/ή η εγκατάσταση λογισμικού που διευκολύνουν την ηλεκτρονική επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν μπορεί να χαρακτηριστεί συγκατάθεση που παρέχεται από τους εργαζομένους, καθώς η συγκατάθεση απαιτεί ενεργό έκφραση της

[9] ΟΕ29, *Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ*, WP217, η οποία εκδόθηκε στις 9 Απριλίου 2014, σύνδεσμος: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_el.pdf.

[10] Σύμφωνα με το άρθρο 11 παράγραφος 2 της οδηγίας για την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση να παράσχει πληροφορίες στο υποκείμενο των δεδομένων σε περιπτώσεις όπου η καταχώριση ή συλλογή δεδομένων επιβάλλεται ρητώς από τον νόμο.

βούλησης. Η μη ανάληψη δράσης (δηλαδή η μη αλλαγή των προεπιλεγμένων ρυθμίσεων) δεν μπορεί, κατά κανόνα, να θεωρηθεί ρητή συγκατάθεση για την εν λόγω επεξεργασία[11].

- **Εκτέλεση σύμβασης [άρθρο 7 στοιχείο β)]**

Οι σχέσεις εργασίας βασίζονται συχνά σε σύμβαση εργασίας μεταξύ του εργοδότη και του εργαζομένου. Κατά την εκπλήρωση των υποχρεώσεων που απορρέουν από τη σύμβαση αυτή, όπως η καταβολή στον εργαζόμενο των αποδοχών του, ο εργοδότης χρειάζεται να προβαίνει στην επεξεργασία ορισμένων δεδομένων προσωπικού χαρακτήρα.

- **Εκ του νόμου υποχρέωση [άρθρο 7 στοιχείο γ)]**

Είναι αρκετά σύνηθες να επιβάλλει η εργατική νομοθεσία υποχρεώσεις στον εργοδότη, στο πλαίσιο των οποίων απαιτείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα (π.χ. για σκοπούς υπολογισμού του φόρου και διαχείρισης μισθών). Είναι σαφές ότι σε τέτοιες περιπτώσεις, ο σχετικός νόμος αποτελεί τη νομική βάση για την επεξεργασία των δεδομένων.

- **Έννομο συμφέρον [άρθρο 7 στοιχείο στ)]**

Αν ο εργοδότης επιθυμεί να στηριχθεί στη νομική βάση του άρθρου 7 στοιχείο στ) της ΟΠΔ, ο σκοπός της επεξεργασίας πρέπει να είναι νόμιμος, και η επιλεγείσα μέθοδος ή ειδική τεχνολογία με την οποία θα πραγματοποιηθεί η επεξεργασία πρέπει να είναι απαραίτητη για το έννομο συμφέρον του εργοδότη. Η επεξεργασία πρέπει επίσης να είναι ανάλογη προς τις ανάγκες της επιχείρησης, δηλαδή προς τον επιδιωκόμενο σκοπό. Η επεξεργασία δεδομένων στην εργασία θα πρέπει να διενεργείται με τον λιγότερο δυνατόν παρεμβατικό τρόπο και να επικεντρώνεται στον συγκεκριμένο τομέα κινδύνου. Επιπλέον, σε περίπτωση επίκλησης του άρθρου 7 στοιχείο στ), ο εργαζόμενος διατηρεί το δικαίωμα να αντιταχθεί στην επεξεργασία για επιτακτικούς και νόμιμους λόγους, σύμφωνα με το άρθρο 14.

Προκειμένου να γίνει επίκληση του άρθρου 7 στοιχείο στ) ως νομική βάση επεξεργασίας, είναι απαραίτητο να υπάρχουν ειδικά μέτρα μετριασμού ώστε να διασφαλίζεται η δίκαιη ισορροπία μεταξύ του έννομου συμφέροντος του εργοδότη και των θεμελιωδών δικαιωμάτων και ελευθεριών των εργαζομένων[12]. Τα μέτρα αυτά, ανάλογα με τη μορφή της παρακολούθησης, θα πρέπει να περιλαμβάνουν περιορισμούς της παρακολούθησης ώστε να διασφαλίζεται ότι δεν θα παραβιάζεται η ιδιωτικότητα του εργαζομένου. Οι περιορισμοί αυτοί θα μπορούσαν να είναι:

- γεωγραφικοί (π.χ. παρακολούθηση μόνο σε συγκεκριμένους χώρους· η παρακολούθηση ευαίσθητων χώρων όπως θρησκευτικοί τόποι και, για παράδειγμα, ζώνες υγιεινής και αίθουσες διαλείμματος, θα πρέπει να απαγορεύεται).

[11] Βλέπε επίσης ΟΕ29, *Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης*, WP187, 13 Ιουλίου 2011, σύνδεσμος: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_el.pdf, σελίδα 24.

[12] Για ένα παράδειγμα της ισορροπίας που πρέπει να επιτευχθεί, βλ. υπόθεση *Köpke κατά Γερμανίας*, [2010], ΕΣΔΑ 1725 (σύνδεσμος: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), όπου εργαζόμενος απολύθηκε ως αποτέλεσμα επιχείρησης κρυφής βιντεοπαρακολούθησης, την οποία είχε θέσει σε εφαρμογή ο εργοδότης και γραφείο ιδιωτικών ερευνών. Ενώ στη συγκεκριμένη περίπτωση το δικαστήριο κατέληξε στο συμπέρασμα ότι οι εθνικές αρχές είχαν πετύχει μια δίκαιη ισορροπία μεταξύ του έννομου συμφέροντος του εργοδότη (κατά την προστασία των δικαιωμάτων ιδιοκτησίας του), του δικαιώματος του εργαζόμενου στο σεβασμό της ιδιωτικής ζωής και του δημόσιου συμφέροντος κατά την απονομή δικαιοσύνης, παρατήρησε επίσης ότι θα μπορούσε να δοθεί διαφορετική βαρύτητα στα διάφορα σχετικά συμφέροντα ως αποτέλεσμα της τεχνολογικής εξέλιξης.

- προσανατολισμένοι στα δεδομένα (π.χ. προσωπικά ηλεκτρονικά αρχεία και επικοινωνίες δεν θα πρέπει να παρακολουθούνται) και
- χρονικοί (π.χ. δειγματοληψία αντί συνεχούς παρακολούθησης).

3.1.2 *ΔΙΑΦΑΝΕΙΑ (ΑΡΘΡΑ 10 ΚΑΙ 11)*

Οι απαιτήσεις διαφάνειας των άρθρων 10 και 11 εφαρμόζονται στην επεξεργασία δεδομένων στην εργασία· οι εργαζόμενοι πρέπει να ενημερώνονται για την ύπαρξη τυχόν παρακολούθησης, τους σκοπούς επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και κάθε άλλη πληροφορία που απαιτείται για τη διασφάλιση της θεμιτής επεξεργασίας.

Με τις νέες τεχνολογίες, η ανάγκη για διαφάνεια καθίσταται εμφανέστερη δεδομένου ότι οι τεχνολογίες αυτές επιτρέπουν τη συλλογή και περαιτέρω επεξεργασία ενδεχομένως τεράστιου όγκου δεδομένων προσωπικού χαρακτήρα με συγκεκαλυμμένο τρόπο.

3.1.3 *ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΕΣ ΑΠΟΦΑΣΕΙΣ (ΑΡΘΡΟ 15)*

Το άρθρο 15 της ΟΠΔ δίνει επίσης στα υποκείμενα των δεδομένων το δικαίωμα να μη συμμορφώνονται με απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, όταν η απόφαση αυτή παράγει έννομα αποτελέσματα ή θίγει σημαντικά τα εν λόγω υποκείμενα των δεδομένων με παρόμοιο τρόπο, και η απόφαση βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία που αξιολογεί ορισμένες πτυχές της προσωπικότητάς τους, όπως η απόδοσή τους στην εργασία, εκτός εάν η απόφαση είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης εγκεκριμένης από την ενωσιακή νομοθεσία ή τη νομοθεσία του κράτους μέλους, ή βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

3.2 Κανονισμός 2016/679 – Γενικός κανονισμός για την προστασία των δεδομένων («ΓΚΠΔ»)

Ο ΓΚΠΔ περιλαμβάνει και ενισχύει τις απαιτήσεις της ΟΠΔ. Εισάγει επίσης νέες υποχρεώσεις για όλους τους υπεύθυνους επεξεργασίας, συμπεριλαμβανομένων των εργοδοτών.

3.2.1 *ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΗΔΗ ΑΠΟ ΤΟ ΣΤΑΔΙΟ ΤΟΥ ΣΧΕΔΙΑΣΜΟΥ*

Το άρθρο 25 του ΓΚΠΔ απαιτεί από τους υπεύθυνους εργασίας να εφαρμόζουν προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Για παράδειγμα: όταν ένας εργοδότης παρέχει συσκευές στους εργαζομένους, θα πρέπει να επιλέγονται οι λύσεις που προστατεύουν περισσότερο την ιδιωτικότητα σε περίπτωση χρήσης τεχνολογιών παρακολούθησης. Πρέπει επίσης να λαμβάνεται υπόψη η ελαχιστοποίηση των δεδομένων.

3.2.2 *ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ*

Το άρθρο 35 του ΓΚΠΔ περιγράφει τις απαιτήσεις για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (ΕΑΠΔ) από τον υπεύθυνο επεξεργασίας, όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να ενέχει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Ένα σχετικό παράδειγμα είναι περίπτωση συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία,

περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο.

Αν η ΕΑΠΔ δείξει ότι οι προσδιορισμένοι κίνδυνοι δεν μπορούν να αντιμετωπιστούν επαρκώς από τον υπεύθυνο επεξεργασίας –δηλαδή ότι ο υπολειπόμενος κίνδυνος παραμένει υψηλός– ο υπεύθυνος επεξεργασίας πρέπει να ζητήσει τη γνώμη της εποπτικής αρχής πριν από την έναρξη της επεξεργασίας (άρθρο 36 παράγραφος 1), όπως ξεκαθαρίζεται στις κατευθυντήριες γραμμές της ΟΕ29 για τις εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων[13].

3.2.2 *«Επεξεργασία στο πλαίσιο της απασχόλησης»*

Το άρθρο 88 του ΓΚΠΔ ορίζει ότι τα κράτη μέλη, μέσω της νομοθεσίας ή μέσω των συλλογικών συμβάσεων, μπορούν να θεσπίζουν ειδικούς κανόνες προκειμένου να διασφαλίζουν την προστασία των δικαιωμάτων και των ελευθεριών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης. Συγκεκριμένα, οι κανόνες αυτοί μπορούν να θεσπίζονται 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·
- άσκησης και απόλαυσης (σε ατομική βάση) δικαιωμάτων και παροχών που σχετίζονται με την απασχόληση· και
- καταγγελίας της σχέσης απασχόλησης.

Σύμφωνα με το άρθρο 88 παράγραφος 2, οι εν λόγω κανόνες θα πρέπει να περιλαμβάνουν κατάλληλα και ειδικά μέτρα για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας, των έννομων συμφερόντων και των θεμελιωδών δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα, με ιδιαίτερη έμφαση στα εξής:

- στη διαφάνεια της επεξεργασίας·
- στη διαβίβαση δεδομένων προσωπικού χαρακτήρα εντός ομίλου επιχειρήσεων, ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα· και
- στα συστήματα παρακολούθησης στο χώρο εργασίας.

Στην παρούσα γνώμη, η ομάδα εργασίας παρέχει κατευθυντήριες γραμμές για τη νόμιμη χρήση των νέων τεχνολογιών σε διάφορες ειδικές καταστάσεις, αναφέροντας κατάλληλα και ειδικά μέτρα για τη διαφύλαξη της ανθρώπινης αξιοπρέπειας, των εννόμων συμφερόντων και των θεμελιωδών δικαιωμάτων των εργαζομένων.

[13] ΟΕ29, *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679*, WP 248, 4 Απριλίου 2017, σύνδεσμος. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, σελίδα 18.

4. Κίνδυνοι

Οι σύγχρονες τεχνολογίες παρέχουν τη δυνατότητα παρακολούθησης των εργαζομένων σε βάθος χρόνου, σε διάφορους χώρους εργασίας και στην οικία τους, μέσω πολλών διαφορετικών συσκευών όπως τα έξυπνα τηλέφωνα, οι επιτραπέζιοι υπολογιστές, οι ταμπλέτες, τα οχήματα και οι φορέσιμες συσκευές. Αν δεν υπάρχουν όρια στην επεξεργασία και αν η επεξεργασία δεν είναι διαφανής, υπάρχει μεγάλος κίνδυνος να μετατραπεί το έννομο συμφέρον των εργοδοτών για τη βελτίωση της αποδοτικότητας και για την προστασία των περιουσιακών στοιχείων της εταιρείας σε αδικαιολόγητη και παρεμβατική παρακολούθηση.

Οι τεχνολογίες παρακολούθησης της επικοινωνίας μπορούν επίσης να έχουν αρνητικό αντίκτυπο στα θεμελιώδη δικαιώματα των εργαζομένων ως προς την οργάνωση, τη σύγκληση συνελεύσεων εργαζομένων και την εμπιστευτική επικοινωνία (συμπεριλαμβανομένου του δικαιώματος στην πληροφόρηση). Η παρακολούθηση των επικοινωνιών και της συμπεριφοράς θα ασκήσει πίεση στους εργαζομένους να συμμορφώνονται με σκοπό να αποτραπεί η ανίχνευση στοιχείων που μπορεί να θεωρηθούν ανωμαλίες, με τρόπο παρόμοιο με αυτόν που η εντατική χρήση της τηλεόρασης κλειστού κυκλώματος έχει επηρεάσει τη συμπεριφορά των πολιτών σε δημόσιους χώρους. Επιπλέον, λόγω των δυνατοτήτων αυτών των τεχνολογιών, οι εργαζόμενοι ενδέχεται να μην γνωρίζουν ποια προσωπικά δεδομένα υφίστανται επεξεργασία και για ποιους σκοπούς, ενώ είναι επίσης πιθανό να μην γνωρίζουν καν την ύπαρξη των ίδιων των τεχνολογιών παρακολούθησης.

Η παρακολούθηση της χρήσης των τεχνολογιών της πληροφορίας διαφέρει επίσης από άλλα, πιο ορατά εργαλεία επιτήρησης και παρακολούθησης, όπως το κλειστό κύκλωμα τηλεόρασης, δεδομένου ότι μπορεί να πραγματοποιηθεί με συγκεκαλυμμένο τρόπο. Ελλείψει μιας ευνόητης και εύκολα προσβάσιμης πολιτικής ως προς την παρακολούθηση στον χώρο εργασίας, οι εργαζόμενοι δεν μπορούν να γνωρίζουν την ύπαρξη και τις συνέπειες της παρακολούθησης που πραγματοποιείται, και επομένως δεν είναι σε θέση να ασκούν τα δικαιώματά τους. Ένας άλλος κίνδυνος προέρχεται από υπερβολική συλλογή δεδομένων στο πλαίσιο των εν λόγω συστημάτων, π.χ. συστημάτων που συλλέγουν δεδομένα θέσης μέσω ασύρματης σύνδεσης (WiFi).

Η αύξηση του όγκου των δεδομένων που παράγονται στο εργασιακό περιβάλλον, σε συνδυασμό με νέες τεχνικές ανάλυσης και διασταύρωσης δεδομένων, μπορεί επίσης να προκαλέσει τον κίνδυνο ασυμβίβαστης περαιτέρω επεξεργασίας. Στα παραδείγματα αθέμιτης περαιτέρω επεξεργασίας περιλαμβάνεται η χρήση συστημάτων νομίμως εγκατεστημένων για την προστασία της περιουσίας με σκοπό την παρακολούθηση της διαθεσιμότητας, της απόδοσης και της φιλικής προς τον πελάτη προσέγγισης των εργαζομένων. Άλλα παραδείγματα περιλαμβάνουν χρήση δεδομένων που συλλέγονται μέσω τηλεόρασης κλειστού κυκλώματος για την τακτική παρακολούθηση της συμπεριφοράς και της απόδοσης των εργαζομένων, ή χρήση στοιχείων ενός συστήματος εντοπισμού γεωγραφικής θέσης (όπως για παράδειγμα εντοπισμό μέσω WiFi ή Bluetooth) με σκοπό τον συνεχή έλεγχο των κινήσεων και της συμπεριφοράς του εργαζόμενου.

Ως εκ τούτου, αυτός ο εντοπισμός ενδέχεται να παραβιάζει τα δικαιώματα των εργαζομένων στην ιδιωτικότητα, ανεξάρτητα από το κατά πόσον η παρακολούθηση πραγματοποιείται συστηματικά ή περιστασιακά. Ο κίνδυνος δεν περιορίζεται στην ανάλυση του περιεχομένου των επικοινωνιών. Ως εκ τούτου, η ανάλυση μεταδεδομένων σχετικά με κάποιο πρόσωπο ενδέχεται να επιτρέπει τη λεπτομερή παρακολούθηση της ζωής του και των μοτίβων συμπεριφοράς του η οποία παραβιάζει εξίσου την ιδιωτικότητα του προσώπου αυτού.

Η εκτεταμένη χρήση των τεχνολογιών παρακολούθησης ενδέχεται επίσης να περιορίσει την προθυμία (και τους διαθέσιμους διαύλους) των εργαζομένων να ενημερώνουν τους εργοδότες σχετικά με παρατυπίες ή παράνομες πράξεις ανωτέρων και/ή άλλων εργαζομένων οι οποίες θα μπορούσαν να βλάψουν την επιχείρηση (ιδιαίτερα τα δεδομένα που αφορούν τον πελάτη) ή τον χώρο εργασίας. Η ανωνυμία είναι συχνά απαραίτητη για να αναλάβει δράση ένας εργαζόμενος με ανησυχίες και να γνωστοποιήσει αντίστοιχες καταστάσεις. Η παρακολούθηση που παραβιάζει τα δικαιώματα των εργαζομένων στην ιδιωτικότητα μπορεί να παρεμποδίσει την απαραίτητη επικοινωνία με τις αρμόδιες αρχές. Σε τέτοιες περιπτώσεις, τα μέσα που έχουν δημιουργηθεί για την εσωτερική καταγγελία δυσλειτουργιών ενδέχεται να καταστούν αναποτελεσματικά[14].

5. Σενάρια

Στην παρούσα ενότητα εξετάζονται διάφορα σενάρια επεξεργασίας δεδομένων στην εργασία, στο πλαίσιο των οποίων οι νέες τεχνολογίες και/ή η ανάπτυξη υφιστάμενων τεχνολογιών έχουν, ή ενδέχεται να έχουν, ως αποτέλεσμα υψηλό κίνδυνο για την ιδιωτικότητα των εργαζομένων. Σε όλες αυτές τις περιπτώσεις, οι εργοδότες θα πρέπει να εξετάζουν κατά πόσο:

- η επεξεργασία είναι απαραίτητη και εάν είναι, την ισχύουσα νομική βάση·
- η προτεινόμενη επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι δίκαιη για τους εργαζόμενους·
- η επεξεργασία είναι ανάλογη προς τις ανησυχίες που εκφράστηκαν· και
- η επεξεργασία είναι διαφανής.

5.1 Επεξεργασία κατά τη διαδικασία πρόσληψης

Η χρήση των μέσων κοινωνικής δικτύωσης από τους ιδιώτες είναι εκτεταμένη και είναι σχετικά σύνηθες προφίλ χρήστη να είναι δημοσίως διαθέσιμα, ανάλογα με τις ρυθμίσεις που έχει επιλέξει ο κάτοχος του λογαριασμού. Ως εκ τούτου, οι εργοδότες μπορεί να πιστεύουν ότι η εξέταση του προφίλ που έχουν οι δυνητικοί υποψήφιοι στα μέσα κοινωνικής δικτύωσης μπορεί να είναι δικαιολογημένη στο πλαίσιο της διαδικασίας πρόσληψης. Το ίδιο μπορεί επίσης να ισχύει για άλλες δημόσια διαθέσιμες πληροφορίες για τον υποψήφιο εργαζόμενο.

Ωστόσο, οι εργοδότες δεν θα πρέπει να υποθέτουν ότι, απλώς και μόνο επειδή το προφίλ ενός προσώπου στα μέσα κοινωνικής δικτύωσης είναι δημόσια διαθέσιμο, επιτρέπεται στους ίδιους να επεξεργαστούν τα δεδομένα αυτά για τους δικούς τους σκοπούς. Για την εν λόγω επεξεργασία απαιτείται νομική βάση, όπως το έννομο συμφέρον. Στο πλαίσιο αυτό, ο εργοδότης –πριν προβεί στην εξέταση ενός προφίλ στα μέσα κοινωνικής δικτύωσης– θα πρέπει να λάβει υπόψη αν το προφίλ του αιτούντος εργασία στα μέσα κοινωνικής δικτύωσης σχετίζεται με επαγγελματικούς ή ιδιωτικούς σκοπούς, καθώς αυτό μπορεί αποτελεί σημαντική ένδειξη για τη νομιμότητα της εξέτασης των δεδομένων. Επιπλέον, οι εργοδότες δικαιούνται να συλλέγουν και να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα που αφορούν τους υποψήφιους για θέση εργασίας μόνο στον βαθμό που η συλλογή των

[14] Βλ., για παράδειγμα, ΟΕ29, *Γνώμη 1/2006 σχετικά με την εφαρμογή των κανόνων της ΕΕ οι οποίοι διέπουν την προστασία των δεδομένων όσον αφορά τις εσωτερικές διαδικασίες καταγγελίας δυσλειτουργιών στους τομείς της λογιστικής, των εσωτερικών λογιστικών ελέγχων, των ελέγχων λογαριασμών, της καταπολέμησης της δωροδοκίας και του τραπεζικού και οικονομικού εγκλήματος*, WP 117, 1 Φεβρουαρίου 2006, σύνδεσμος: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_el.pdf.

δεδομένων αυτών είναι απαραίτητη και σχετική με την εκτέλεση της εργασίας για την οποία υποβάλλεται η αίτηση.

Τα δεδομένα που συλλέγονται κατά τη διάρκεια της διαδικασίας πρόσληψης θα πρέπει γενικώς να διαγράφονται αμέσως μόλις διαπιστωθεί ότι δεν θα γίνει προσφορά εργασίας ή ότι αυτή δεν γίνεται αποδεκτή από το ενδιαφερόμενο πρόσωπο[15]. Το πρόσωπο πρέπει επίσης να λαμβάνει ορθή ενημέρωση ως προς οποιαδήποτε τέτοια επεξεργασία προτού συμμετάσχει στη διαδικασία πρόσληψης.

Δεν δεν υπάρχει νομική βάση που να επιτρέπει σε εργοδότη να απαιτεί από δυνητικούς εργαζόμενους να συνδεθούν με τον δυνητικό εργοδότη στα μέσα κοινωνικής δικτύωσης ή να του παράσχουν με άλλο τρόπο πρόσβαση στο περιεχόμενο των προφίλ τους.

Παράδειγμα

Κατά την πρόσληψη νέων υπαλλήλων, ο εργοδότης ελέγχει τα προφίλ των υποψηφίων σε διάφορα μέσα κοινωνικής δικτύωσης και συμπεριλαμβάνει πληροφορίες από τα δίκτυα αυτά (και τυχόν άλλες πληροφορίες που είναι διαθέσιμες στο διαδίκτυο) στη διαδικασία επιλογής.

Ο εργοδότης ενδέχεται να έχει νομική βάση σύμφωνα με το άρθρο 7 στοιχείο στ) να εξετάσει δημόσια διαθέσιμες πληροφορίες σχετικά με υποψηφίους μόνο αν η εξέταση πληροφοριών στα μέσα κοινωνικής δικτύωσης σχετικά με έναν υποψήφιο είναι απαραίτητη για την εργασία, για παράδειγμα για να καταστεί δυνατή η αξιολόγηση συγκεκριμένων κινδύνων σχετικά με υποψήφιους για συγκεκριμένη εργασία, και οι υποψήφιοι λάβουν ορθή πληροφόρηση (για παράδειγμα, στο κείμενο της αγγελίας για τη θέση εργασίας).

[15] Βλέπε Συμβούλιο της Ευρώπης, *Σύσταση CM/Rec(2015)5 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της εργασίας*, παράγραφος 13.2 (1 Απριλίου 2015). https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). Σε περιπτώσεις όπου ο εργοδότης επιθυμεί να διατηρήσει τα δεδομένα ενόψει περαιτέρω εργασιακής ευκαιρίας, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται σχετικά και να του δίνεται η δυνατότητα εναντίωσης στην εν λόγω περαιτέρω επεξεργασία, οπότε και τα δεδομένα θα πρέπει να διαγράφονται (ό.π.)

5.2 Επεξεργασία που προκύπτει από έλεγχο κατά τη διάρκεια της εργασίας

Μέσω των προφίλ που υπάρχουν στα μέσα κοινωνικής δικτύωσης και της ανάπτυξης νέων αναλυτικών τεχνολογιών, οι εργοδότες έχουν (ή μπορούν να αποκτήσουν) την τεχνική ικανότητα μόνιμου ελέγχου των εργαζομένων, μέσω της συλλογής πληροφοριών σχετικά με τους φίλους, τις απόψεις, τις πεποιθήσεις, τα ενδιαφέροντα, τις συνήθειες, τις κινήσεις, τις στάσεις και τη συμπεριφορά τους, καταγράφοντας ως εκ τούτου δεδομένα για την ιδιωτική και οικογενειακή ζωή του εργαζόμενου, μεταξύ αυτών και ευαίσθητα δεδομένα.

Ο έλεγχος των προφίλ των εργαζομένων στα μέσα κοινωνικής δικτύωσης κατά τη διάρκεια της εργασίας δεν θα πρέπει να λαμβάνει χώρα σε γενικευμένη βάση.

Επιπλέον, οι εργοδότες θα πρέπει να αποφεύγουν να ζητούν από εργαζόμενο ή από υποψήφιο για θέση εργασίας πρόσβαση σε πληροφορίες τις οποίες μοιράζεται με άλλους στα μέσα κοινωνικής δικτύωσης.

Παράδειγμα
Εργοδότης παρακολουθεί το προφίλ στο LinkedIn πρώην εργαζομένων για τους οποίους ισχύει ρήτρα απαγόρευσης ανταγωνισμού. Ο σκοπός της παρακολούθησης είναι να εξακριβωθεί η συμμόρφωση με τις ρήτρες αυτές. Η παρακολούθηση περιορίζεται σε αυτούς τους πρώην εργαζόμενους.

Εφόσον ο εργοδότης μπορεί να αποδείξει ότι η εν λόγω παρακολούθηση είναι απαραίτητη για την προστασία των έννομων συμφερόντων του, ότι δεν υπάρχουν άλλα, λιγότερο παρεμβατικά διαθέσιμα μέσα, και ότι οι πρώην εργαζόμενοι έχουν ενημερωθεί επαρκώς για την έκταση της τακτικής παρακολούθησης των δημόσιων επικοινωνιών τους, ο εργαζόμενος μπορεί να επικαλεστεί τη νομική βάση του άρθρου 7 στοιχείο στ) της ΟΠΔ.

Επιπλέον, δεν θα πρέπει να απαιτείται από τους εργαζόμενους να χρησιμοποιούν προφίλ μέσων κοινωνικής δικτύωσης που παρέχεται από τον εργοδότη τους. Ακόμα και όταν αυτό προβλέπεται ειδικά στο πλαίσιο των καθηκόντων τους (π.χ. εκπρόσωπος οργανισμού), οι εργαζόμενοι θα πρέπει να διατηρούν την επιλογή να έχουν ένα μη δημόσιο προφίλ που δεν σχετίζεται με την εργασία τους και το οποίο μπορούν να χρησιμοποιούν αντί του «επισήμου» προφίλ που σχετίζεται με τον εργοδότη, και αυτό θα πρέπει να διευκρινίζεται στους όρους και τις προϋποθέσεις της σύμβασης εργασίας.

5.3 Επεξεργασία που προκύπτει από την παρακολούθηση της χρήσης ΤΠΕ στον χώρο εργασίας

Παραδοσιακά, η παρακολούθηση των ηλεκτρονικών επικοινωνιών στον χώρο εργασίας (π.χ. τηλέφωνο, περιήγηση στο διαδίκτυο, ηλεκτρονική αλληλογραφία, άμεση ανταλλαγή μηνυμάτων, VOIP κ.λπ.) θεωρούνταν η βασική απειλή για την ιδιωτικότητα των εργαζομένων. Στο *Έγγραφο εργασίας για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας* του 2002, η ΟΕ29 κατέληξε σε έναν αριθμό συμπερασμάτων σχετικά με την παρακολούθηση του ηλεκτρονικού ταχυδρομείου και τη χρήση του διαδικτύου. Ενώ τα συμπεράσματα αυτά παραμένουν έγκυρα, χρειάζεται να ληφθούν υπόψη οι τεχνολογικές εξελίξεις που έχουν δώσει τη δυνατότητα για νέους τρόπους παρακολούθησης, που είναι κατά πάσα πιθανότητα πιο παρεμβατικοί και πιο εκτεταμένοι. Οι εξελίξεις αυτές περιλαμβάνουν, μεταξύ άλλων:

- εργαλεία πρόληψης απώλειας δεδομένων (DLP), που παρακολουθούν τις εξερχόμενες επικοινωνίες με σκοπό τον εντοπισμό ενδεχόμενων παραβιάσεων δεδομένων·
- τείχη προστασίας νέας γενιάς (NGFW) και συστήματα ενιαίας διαχείρισης απειλών (UTM), που μπορούν να παράσχουν μεγάλο εύρος τεχνολογιών παρακολούθησης, στην οποία συμπεριλαμβάνεται ο εις βάθος έλεγχος πακέτων, η παρακολούθηση ασφάλειας επιπέδου μεταφοράς (TLS), το φιλτράρισμα ιστοτόπων, το φιλτράρισμα περιεχομένου, η παραγωγή αναφορών εντός της συσκευής (on-appliance reporting), οι πληροφορίες ταυτότητας του χρήστη και (όπως περιγράφεται ανωτέρω) η πρόληψη απώλειας δεδομένων. Οι τεχνολογίες αυτές μπορούν επίσης να χρησιμοποιούνται σε μεμονωμένη βάση, ανάλογα με τον εργοδότη·
- εφαρμογές και μέτρα ασφαλείας, που περιλαμβάνουν την καταγραφή της πρόσβασης του εργαζόμενου στα συστήματα του εργοδότη·
- τεχνολογία ηλεκτρονικής διερεύνησης στοιχείων, δηλαδή οποιασδήποτε διαδικασίας στο πλαίσιο της οποίας ερευνώνται ηλεκτρονικά δεδομένα με σκοπό τη χρήση τους ως αποδεικτικών στοιχείων·
- παρακολούθηση της χρήσης εφαρμογών και συσκευών μέσω αφανούς λογισμικού, είτε στον υπολογιστή είτε στο υπολογιστικό νέφος·
- χρήση στο χώρο εργασίας εφαρμογών γραφείου που παρέχονται ως υπηρεσία υπολογιστικού νέφους, οι οποίες στη θεωρία επιτρέπουν την πολύ λεπτομερή καταγραφή των δραστηριοτήτων των εργαζομένων·
- παρακολούθηση προσωπικών συσκευών (π.χ. υπολογιστές, κινητά τηλέφωνα, ταμπλέτες) τις οποίες παρέχουν οι εργοδότες στους εργαζομένους στο πλαίσιο της εργασίας τους, σύμφωνα με ειδική πολιτική χρήσης, όπως η χρήση προσωπικών συσκευών (BYOD), καθώς και τεχνολογία διαχείρισης κινητών συσκευών (MDM), η οποία επιτρέπει τη διανομή εφαρμογών, δεδομένων και ρυθμίσεων διαμόρφωσης, καθώς και πρόχειρες διορθώσεις για κινητές συσκευές· και
- χρήση φορετών συσκευών (π.χ. συσκευές υγείας και ευεξίας).

Ενδέχεται ο εργοδότης να εφαρμόσει μια ολοκληρωμένη λύση παρακολούθησης, όπως για παράδειγμα μια οικογένεια πακέτων ασφαλείας που δίνουν τη δυνατότητα να παρακολουθείται το σύνολο της χρήσης των ΤΠΕ στον τόπο εργασίας και όχι μόνο το ηλεκτρονικό ταχυδρομείο και/ή η χρήση ιστοτόπων, όπως κάποτε. Τα συμπεράσματα του εγγράφου εργασίας WP55 ισχύουν για κάθε σύστημα που επιτρέπει την παρακολούθηση αυτού του είδους[16].

Παράδειγμα

Εργοδότης σκοπεύει να αναπτύξει εφαρμογή επιθεώρησης ασφάλειας επιπέδου μεταφοράς (TLS) και να παρακολουθεί την ασφαλή κυκλοφορία, με σκοπό την ανίχνευση τυχόν κακόβουλων περιστατικών. Η συσκευή μπορεί επίσης να καταγράφει και να αναλύει το σύνολο της ηλεκτρονικής δραστηριότητας του εργαζόμενου στο δίκτυο της εταιρείας.

[16] Βλ. επίσης υπόθεση *Copland κατά Ηνωμένου Βασιλείου* (2007), EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (σύνδεσμος: http://www.bailii.org/eu/cases/ECHR/2007/253.html), στην οποία το δικαστήριο δήλωσε ότι ηλεκτρονικά μηνύματα που αποστέλλονται από επαγγελματικές εγκαταστάσεις και πληροφορίες που προκύπτουν από την παρακολούθηση της χρήσης του διαδικτύου θα μπορούσαν να αποτελούν μέρος της ιδιωτικής ζωής και αλληλογραφίας του εργαζόμενου και ότι η συλλογή και αποθήκευση των εν λόγω πληροφοριών εν αγνοία του εργαζομένου ισοδυναμούν με προσβολή των δικαιωμάτων του εργαζομένου, παρόλο που το δικαστήριο δεν αποφάνθηκε ότι παρακολούθηση αυτού του είδους δεν θα ήταν ποτέ απαραίτητη σε μια δημοκρατική κοινωνία.

Η χρήση πρωτοκόλλων κρυπτογραφημένης επικοινωνίας χρησιμοποιείται ολοένα και συχνότερα για την προστασία από υποκλοπή των ηλεκτρονικών ροών δεδομένων που αφορούν δεδομένα προσωπικού χαρακτήρα. Ωστόσο, αυτό μπορεί επίσης να ενέχει προβλήματα, καθώς η κρυπτογράφηση καθιστά αδύνατη την παρακολούθηση των εισερχόμενων και εξερχόμενων δεδομένων. Ο εξοπλισμός παρακολούθησης TLS αποκρυπτογραφεί τη ροή των δεδομένων, αναλύει το περιεχόμενο για σκοπούς ασφαλείας και στη συνέχεια κρυπτογραφεί εκ νέου τη ροή.

Στο παράδειγμα αυτό, ο εργοδότης στηρίζεται σε έννομα συμφέροντα – την ανάγκη προστασίας του δικτύου και των δεδομένων προσωπικού χαρακτήρα των εργαζομένων και των πελατών τα οποία διατηρούνται στο δίκτυο αυτό από τη μη εξουσιοδοτημένη πρόσβαση ή τη διαρροή δεδομένων. Ωστόσο, η παρακολούθηση κάθε ηλεκτρονικής δραστηριότητας των εργαζομένων είναι δυσανάλογη αντίδραση και θίγει το δικαίωμα στο απόρρητο των επικοινωνιών. Ο εργοδότης θα πρέπει πρώτα να εξετάζει το ενδεχόμενο χρήσης άλλων, λιγότερο επεμβατικών μέσων προστασίας της εμπιστευτικότητας των δεδομένων των πελατών και της ασφάλειας του δικτύου.

Στο βαθμό που κάποια παρακολούθηση της κυκλοφορίας TLS μπορεί να χαρακτηριστεί απολύτως απαραίτητη, η συσκευή θα πρέπει να διαμορφώνεται με τέτοιον τρόπο ώστε να μην επιτρέπεται η μόνιμη καταγραφή της δραστηριότητας του εργαζόμενου, παραδείγματος χάριν μέσω του αποκλεισμού της ύποπτης εισερχόμενης ή εξερχόμενης κυκλοφορίας και της ανακατεύθυνσης του χρήστη σε διαδικτυακή πύλη πληροφόρησης στην οποία μπορεί να ζητήσει την επανεξέταση της αυτοματοποιημένης απόφασης. Αν, παρόλα αυτά, θεωρηθεί απολύτως απαραίτητος ένας βαθμός γενικής καταγραφής, η συσκευή μπορεί επίσης να διαμορφωθεί έτσι ώστε να μην αποθηκεύει δεδομένα καταγραφής, εκτός αν η συσκευή παραγάγει ειδοποίηση για περιστατικό, ελαχιστοποιώντας τις συλλεγόμενες πληροφορίες.

Ως καλή πρακτική, ο εργοδότης θα μπορούσε να προσφέρει στους εργαζομένους εναλλακτική, μη παρακολουθούμενη πρόσβαση. Αυτό θα μπορούσε να επιτευχθεί μέσω της παροχής δωρεάν ασύρματου τοπικού δικτύου (WiFi), ή αυτόνομες συσκευές ή τερματικά (με κατάλληλες διασφαλίσεις για την εμπιστευτικότητα των επικοινωνιών), όπου οι εργαζόμενοι μπορούν να ασκήσουν το νόμιμο δικαίωμά τους να χρησιμοποιούν τις εγκαταστάσεις της εργασίας τους για ιδιωτική χρήση, ως ένα βαθμό[17]. Επιπλέον, οι εργοδότες θα πρέπει να εξετάζουν ορισμένους τύπους κυκλοφορίας η παρακολούθηση της οποίας θέτει σε κίνδυνο την ορθή ισορροπία μεταξύ των έννομων συμφερόντων τους και της ιδιωτικότητας των εργαζομένων – όπως η χρήση ιδιωτικού διαδικτυακού ταχυδρομείου, επισκέψεις σε ιστότοπους ηλεκτρονικής τραπεζικής και υγείας– με σκοπό την κατάλληλη διαμόρφωση της συσκευής ώστε να μην διενεργεί παρακολούθηση επικοινωνιών σε περιπτώσεις που αυτές δεν εντάσσονται στο πλαίσιο της αναλογικότητας. Θα πρέπει να διευκρινίζονται στους εργαζόμενους πληροφορίες για το είδος των επικοινωνιών που παρακολουθεί η συσκευή.

[17] Βλ. απόφαση στην υπόθεση *Halford κατά Ηνωμένου Βασιλείου*, [1997] ECHR 32, (σύνδεσμος: http://www.bailii.org/eu/cases/ECHR/1997/32.html), στην οποία το δικαστήριο έκρινε ότι «οι τηλεφωνικές κλήσεις που διενεργούνται από επαγγελματικό χώρο καθώς και από την οικία ενδέχεται να καλύπτονται από τις έννοιες "ιδιωτική ζωή" και "αλληλογραφία" υπό την έννοια του άρθρου 8 παράγραφος 1 [της Σύμβασης]»· και *Barbulescu κατά Ρουμανίας*, [2016] ECHR 61, (σύνδεσμος: http://www.bailii.org/eu/cases/ECHR/2016/61.html), σχετικά με τη χρήση επαγγελματικού λογαριασμού σε υπηρεσία ανταλλαγής άμεσων μηνυμάτων για προσωπική αλληλογραφία, όπου το δικαστήριο έκρινε ότι η παρακολούθηση του λογαριασμού από τον εργοδότη ήταν περιορισμένη και αναλογική· η μειοψηφούσα γνώμη ήταν του δικαστή Pinto de Alberquerque, σύμφωνα με την οποία θα έπρεπε να επιτευχθεί μια λεπτή ισορροπία.

Θα πρέπει να δημιουργηθεί μια πολιτική ως προς το πότε και από ποιον μπορούν να προσπελαύνονται ύποπτα δεδομένα, η οποία θα είναι εύκολα και μόνιμα προσπελάσιμη από όλους τους εργαζομένους, και σκοπός της θα είναι, μεταξύ άλλων, να τους παρέχει καθοδήγηση για την αποδεκτή και μη αποδεκτή χρήση του δικτύου και των εγκαταστάσεων. Αυτό επιτρέπει στους εργαζόμενους να προσαρμόζουν τη συμπεριφορά τους ώστε να αποφεύγουν την παρακολούθηση όταν χρησιμοποιούν νομίμως τις εγκαταστάσεις πληροφορικής της εργασίας τους για ιδιωτική χρήση. Ως καλή πρακτική, η πολιτική αυτή θα πρέπει να αξιολογείται, τουλάχιστον σε ετήσια βάση, ώστε να εκτιμάται κατά πόσον η επιλεγείσα λύση παρακολούθησης αποδίδει τα επιδιωκόμενα αποτελέσματα και αν υπάρχουν άλλα, λιγότερο παρεμβατικά, διαθέσιμα εργαλεία ή μέσα για την επίτευξη των ίδιων σκοπών.

Ανεξαρτήτως της οικείας τεχνολογίας ή των δυνατοτήτων της, η νομική βάση του άρθρου 7 στοιχείο στ) είναι διαθέσιμη μόνο αν η επεξεργασία πληροί ορισμένες προϋποθέσεις. Πρώτον, οι εργοδότες που χρησιμοποιούν αυτά τα προϊόντα και τις εφαρμογές πρέπει να εξετάζουν την αναλογικότητα των μέτρων που εφαρμόζουν, και κατά πόσον μπορούν να αναληφθούν περαιτέρω δράσεις για τον μετριασμό ή τη μείωση της κλίμακας και των επιπτώσεων της επεξεργασίας δεδομένων. Ως παράδειγμα ορθής πρακτικής, η εν λόγω εξέταση μπορεί να πραγματοποιηθεί μέσω ΕΕΠΔ πριν από τη χρήση οποιασδήποτε τεχνολογίας παρακολούθησης. Δεύτερον, μαζί με τις πολιτικές απορρήτου, οι εργοδότες πρέπει να εφαρμόζουν και να γνωστοποιούν πολιτικές αποδεκτής χρήσης, οι οποίες θα περιγράφουν την επιτρεπόμενη χρήση των δικτύων και του εξοπλισμού της εταιρείας και θα περιγράφουν λεπτομερώς την πραγματοποιούμενη επεξεργασία.

Σε ορισμένες χώρες, η δημιουργία μιας τέτοιας πολιτικής προϋποθέτει από τον νόμο την έγκριση από επιτροπή εργαζομένων ή παρόμοιο όργανο εκπροσώπησης των εργαζομένων. Στην πράξη, αυτές οι πολιτικές συχνά συντάσσονται από το προσωπικό συντήρησης των πληροφοριακών συστημάτων. Δεδομένου ότι το εν λόγω προσωπικό εστιάζει ως επί το πλείστον στην ασφάλεια και όχι στη θεμιτή προσδοκία των εργαζομένων για σεβασμό της ιδιωτικότητάς τους, η ΟΕ29 συνιστά σε κάθε περίπτωση να εμπλέκεται στην αξιολόγηση της αναγκαιότητας της παρακολούθησης καθώς και τη λογική και την προσβασιμότητα της πολιτικής ένα αντιπροσωπευτικό δείγμα των εργαζομένων.

Παράδειγμα

Εργοδότης θέτει σε εφαρμογή εργαλείο πρόληψης απώλειας δεδομένων για την αυτόματη παρακολούθηση των εξερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου, με σκοπό την πρόληψη της μη εξουσιοδοτημένης διαβίβασης ιδιόκτητων δεδομένων (π.χ. δεδομένα προσωπικού χαρακτήρα πελάτη), ανεξάρτητα από το κατά πόσον μια τέτοια ενέργεια είναι ή όχι ακούσια. Όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου θεωρηθεί ως η πιθανή πηγή παραβίασης δεδομένων, διενεργείται περαιτέρω έρευνα.

Και σε αυτήν την περίπτωση, ο εργοδότης επικαλείται την ανάγκη προάσπισης του έννομου συμφέροντός του να προστατέψει τα δεδομένα προσωπικού χαρακτήρα των πελατών του, καθώς και τα περιουσιακά στοιχεία του, κατά της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα ή της διαρροής δεδομένων. Ωστόσο, αυτό το εργαλείο πρόληψης απώλειας δεδομένων ενδέχεται να συνεπάγεται περιττή επεξεργασία δεδομένων προσωπικού χαρακτήρα – για παράδειγμα, μια «ψευδώς θετική» ειδοποίηση ενδέχεται να έχει ως αποτέλεσμα τη μη εξουσιοδοτημένη πρόσβαση σε θεμιτά μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία έχουν σταλεί από εργαζόμενους (τα οποία μπορεί να είναι, για παράδειγμα, προσωπικά μηνύματα ηλεκτρονικού ταχυδρομείου).

Ως εκ τούτου, η αναγκαιότητα και η χρήση του εργαλείου πρόληψης απώλειας δεδομένων θα πρέπει να αιτιολογούνται πλήρως ώστε να επιτυγχάνεται η ορθή ισορροπία μεταξύ των έννομων συμφερόντων του εργοδότη και του θεμελιώδους δικαιώματος της προστασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων. Για να είναι δυνατή η επίκληση των έννομων συμφερόντων του εργοδότη, θα πρέπει να λαμβάνονται ορισμένα μέτρα μετριασμού του κινδύνου. Για παράδειγμα, οι κανόνες τους οποίους ακολουθεί το σύστημα για να χαρακτηρίσει ένα μήνυμα ηλεκτρονικού ταχυδρομείου ως ενδεχόμενη παραβίαση δεδομένων θα πρέπει να είναι απολύτως διαφανείς για τους χρήστες, και σε περιπτώσεις που το εργαλείο αναγνωρίσει ένα προς αποστολή μήνυμα ηλεκτρονικού ταχυδρομείου ως ενδεχόμενη παραβίαση δεδομένων, ο αποστολέας θα πρέπει να λαμβάνει προειδοποιητικό μήνυμα πριν από την αποστολή του μηνύματος ηλεκτρονικού ταχυδρομείου, έτσι ώστε να του δίνεται η δυνατότητα να ακυρώσει την αποστολή.

Σε ορισμένες περιπτώσεις, η παρακολούθηση των εργαζομένων είναι εφικτή όχι τόσο λόγω της χρήσης ειδικών τεχνολογιών αλλά απλώς επειδή οι εργαζόμενοι χρειάζεται να χρησιμοποιούν ηλεκτρονικές εφαρμογές που διατίθενται από τον εργοδότη, οι οποίες επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Σχετικό παράδειγμα είναι η χρήση εφαρμογών γραφείου υπολογιστικού νέφους (π.χ. επεξεργαστές κειμένου, ημερολόγια, εφαρμογές κοινωνικής δικτύωσης). Θα πρέπει να διασφαλίζεται ότι οι εργαζόμενοι μπορούν να ορίσουν συγκεκριμένα ιδιωτικά τμήματα στα οποία ο εργοδότης δεν μπορεί να έχει πρόσβαση παρά μόνο υπό εξαιρετικές περιστάσεις. Αυτό, για παράδειγμα, αφορά τα ημερολόγια, τα οποία συχνά χρησιμοποιούνται και για ιδιωτικά ραντεβού. Αν ο εργαζόμενος χαρακτηρίζει ένα ραντεβού ως «ιδιωτικό» ή περιλάβει σχετική σημείωση στο ίδιο το ραντεβού, ο εργοδότης (και οι άλλοι εργαζόμενοι) δεν θα πρέπει να έχουν τη δυνατότητα να δουν το περιεχόμενο του ραντεβού.

Η απαίτηση για αναλογικότητα στο πλαίσιο αυτό ορισμένες φορές σημαίνει ότι δεν μπορεί να λαμβάνει χώρα κανενός είδους παρακολούθηση. Για παράδειγμα, αυτό ισχύει στην περίπτωση που η απαγορευμένη χρήση υπηρεσιών επικοινωνιών μπορεί να προληφθεί με τον αποκλεισμό ορισμένων ιστοτόπων. Αν υπάρχει η δυνατότητα αποκλεισμού ιστοτόπου αντί της συνεχούς παρακολούθησης όλων των επικοινωνιών, θα πρέπει να επιλέγεται ο αποκλεισμός ώστε να επιτυγχάνεται η συμμόρφωση με την απαίτηση επικουρικότητας.

Γενικότερα, θα πρέπει να δίνεται πολύ μεγαλύτερη βαρύτητα στην πρόληψη από ό,τι στον εντοπισμό – τα συμφέροντα του εργοδότη εξυπηρετούνται καλύτερα με την πρόληψη της κατάχρησης του διαδικτύου με τεχνικά μέσα από ό,τι με τη δαπάνη πόρων για τον εντοπισμό της κατάχρησης.

5.4 Επεξεργασία που προκύπτει από την παρακολούθηση της χρήσης ΤΠΕ εκτός του χώρου εργασίας

Η χρήση ΤΠΕ εκτός του χώρου εργασίας έχει αυξηθεί με την ανάπτυξη των πολιτικών εργασίας από το σπίτι, τηλεεργασίας και «χρήσης προσωπικών συσκευών». Οι δυνατότητες των τεχνολογιών αυτών μπορούν να αποτελέσουν κίνδυνο για την ιδιωτική ζωή των εργαζομένων, καθώς σε πολλές περιπτώσεις τα συστήματα παρακολούθησης που υπάρχουν στον χώρο εργασίας επεκτείνονται ουσιαστικά στην οικιακή σφαίρα των εργαζομένων, όταν οι εργαζόμενοι χρησιμοποιούν τον εν λόγω εξοπλισμό.

5.4.1 *ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΤΗΣ ΚΑΤ' ΟΙΚΟΝ ΕΡΓΑΣΙΑΣ ΚΑΙ ΤΗΣ ΤΗΛΕΕΡΓΑΣΙΑΣ*

Έχει γίνει συνηθέστερο να προσφέρουν οι εργοδότες στους εργαζόμενους τη δυνατότητα τηλεεργασίας, π.χ. από το σπίτι και/ή ενώ ταξιδεύουν. Πράγματι, αυτό αποτελεί βασικό παράγοντα για την άμβλυνση της διάκρισης μεταξύ του χώρου εργασίας και της οικίας. Σε γενικές γραμμές, σε αυτό το πλαίσιο ο εργοδότης χορηγεί στους εργαζόμενους εξοπλισμό ή λογισμικό πληροφορικής που, όταν εγκατασταθεί στην οικία τους/στις συσκευές τους, τους δίνει τη δυνατότητα να έχουν το ίδιο επίπεδο πρόσβασης στο δίκτυο, τα συστήματα και τους πόρους του εργοδότη που θα είχαν και στο χώρο εργασίας, ανάλογα με την εφαρμογή.

Ενώ η τηλεργασία μπορεί να αποτελέσει θετική εξέλιξη, παρουσιάζει επίσης πρόσθετο κίνδυνο για τον εργοδότη. Για παράδειγμα, εργαζόμενοι που έχουν απομακρυσμένη πρόσβαση στην υποδομή του εργοδότη δεν δεσμεύονται από τα μέτρα υλικής ασφάλειας που ενδέχεται να υπάρχουν στις εγκαταστάσεις του εργοδότη. Με λίγα λόγια: χωρίς την εφαρμογή κατάλληλων τεχνικών μέτρων, αυξάνεται ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης και ενδέχεται να έχει ως αποτέλεσμα την απώλεια ή την καταστροφή πληροφοριών που ενδέχεται να έχει ο εργοδότης, συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα εργαζομένων ή πελατών.

Για να μετριαστεί ο εν λόγω τομέας κινδύνου, οι εργοδότες ενδέχεται να θεωρούν ότι είναι δικαιολογημένη η χρήση πακέτων λογισμικού (είτε επιτόπου είτε στο υπολογιστικό νέφος) που έχουν τη δυνατότητα, παραδείγματος χάριν, καταγραφής της ακολουθίας χαρακτήρων πληκτρολογίου και των κινήσεων του ποντικού, καταγραφής στιγμιότυπων οθόνης (είτε σε τυχαία είτε σε τακτά διαστήματα), καταγραφής των χρησιμοποιούμενων εφαρμογών (και του χρόνου χρήσης τους), και, σε συμβατές συσκευές, ενεργοποίησης διαδικτυακών καμερών και συλλογής του μαγνητοσκοπημένου υλικού. Οι τεχνολογίες αυτές είναι ευρέως διαθέσιμες, μεταξύ άλλων και από τρίτους, όπως οι πάροχοι υπηρεσιών υπολογιστικού νέφους.

Ωστόσο, η επεξεργασία που διενεργείται στο πλαίσιο των εν λόγω τεχνολογιών είναι δυσανάλογη και είναι πολύ απίθανο να έχει ο εργοδότης νομική βάση στο πλαίσιο έννομου συμφέροντος όσον αφορά, παραδείγματος χάριν, την καταγραφή της ακολουθίας χαρακτήρων πληκτρολογίου και κινήσεων ποντικιού.

Το κλειδί είναι να αντιμετωπιστεί ο κίνδυνος που απορρέει από την κατ' οίκον εργασία και την τηλεεργασία με αναλογικό, μη υπερβολικό τρόπο, με όποιον τρόπο και εάν παρέχεται η

δυνατότητα και όποια και αν είναι η τεχνολογία που προτείνεται, ιδίως αν τα όρια μεταξύ επαγγελματικής και ιδιωτικής χρήσης είναι ρευστά.

5.4.2 *ΧΡΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΣΥΣΚΕΥΩΝ (BYOD)*

Λόγω της αύξησης της δημοτικότητας, των χαρακτηριστικών και των δυνατοτήτων που έχουν οι καταναλωτικές ηλεκτρονικές συσκευές, οι εργαζόμενοι ενδέχεται να ζητήσουν από τον εργοδότη να χρησιμοποιούν τις δικές τους συσκευές στο χώρο εργασίας για την εκτέλεση των καθηκόντων τους. Η τακτική αυτή είναι γνωστή ως «χρήση προσωπικών συσκευών».

Η αποτελεσματική υλοποίηση της χρήσης προσωπικών συσκευών μπορεί να έχει μια σειρά από οφέλη για τους εργαζομένους, στα οποία περιλαμβάνεται η βελτίωση της ικανοποίησης από την εργασία, η συνολική αύξηση του ηθικού, η αυξημένη αποτελεσματικότητα στην εργασία και η αυξημένη ευελιξία. Ωστόσο, εξ ορισμού, η χρήση της συσκευής από τον εργαζόμενο θα είναι, ως ένα βαθμό, προσωπικής φύσης, και αυτό είναι πιθανότερο να συμβαίνει σε ορισμένες ώρες της ημέρας (π.χ. βραδινές ώρες και σαββατοκύριακα). Ως εκ τούτου, είναι σαφώς πιθανό η χρήση από τους εργαζόμενους των συσκευών τους να έχει ως αποτέλεσμα την επεξεργασία από τους εργοδότες μη εταιρικών πληροφοριών για τους εργαζομένους αλλά και ενδεχομένως για μέλη της οικογένειάς τους που επίσης χρησιμοποιούν τις εν λόγω συσκευές.

Στο πλαίσιο της εργασίας, οι κίνδυνοι για την ιδιωτικότητα τους οποίους ενέχει η χρήση προσωπικών συσκευών συνδέονται συνήθως με τεχνολογίες παρακολούθησης που συλλέγουν αναγνωριστικά στοιχεία όπως διευθύνσεις MAC, ή με περιπτώσεις στις οποίες ο εργοδότης προσπελαύνει συσκευή του εργαζομένου με τη δικαιολογία της διενέργειας σάρωσης ασφαλείας, δηλαδή σάρωση για την ανίχνευση κακόβουλου λογισμικού. Όσον αφορά το τελευταίο, υπάρχουν διάφορες εμπορικές λύσεις που επιτρέπουν τη σάρωση ιδιωτικών συσκευών, ωστόσο η χρήση τους θα μπορούσε ενδεχομένως να οδηγήσει στην προσπέλαση όλων των δεδομένων στη συγκεκριμένη συσκευή και ως εκ τούτου οι λύσεις αυτές θα πρέπει να τυγχάνουν προσεκτικής διαχείρισης. Για παράδειγμα, δεν επιτρέπεται καταρχήν η προσπέλαση των τμημάτων συσκευής τα οποία τεκμαίρεται ότι χρησιμοποιούνται μόνο για ιδιωτικούς σκοπούς (π.χ. ο φάκελος αποθήκευσης φωτογραφιών που λαμβάνονται με τη συσκευή).

Η παρακολούθηση της θέσης και της κυκλοφορίας των συσκευών αυτών μπορεί να θεωρηθεί ότι εξυπηρετεί το έννομο συμφέρον προστασίας των προσωπικών δεδομένων των οποίων ο εργοδότης, ως υπεύθυνος επεξεργασίας, έχει την ευθύνη· ωστόσο, αυτό μπορεί να είναι παράνομο όσον αφορά τη συσκευή του εργαζομένου, αν η εν λόγω παρακολούθηση συλλέγει επίσης δεδομένα που σχετίζονται με την ιδιωτική και οικογενειακή ζωή του εργαζόμενου. Προκειμένου να αποτραπεί η παρακολούθηση ιδιωτικών πληροφοριών, πρέπει να εφαρμόζονται κατάλληλα μέτρα με σκοπό τη διάκριση μεταξύ της ιδιωτικής και της επαγγελματικής χρήσης της συσκευής.

Οι εργοδότες θα πρέπει επίσης να εφαρμόζουν μεθόδους με τις οποίες τα δικά τους δεδομένα που υπάρχουν στη συσκευή διαβιβάζονται με ασφάλεια μεταξύ της συσκευής και του δικτύου τους. Ενδέχεται επομένως η συσκευή να είναι διαμορφωμένη έτσι ώστε να δρομολογεί όλη την κυκλοφορία μέσω VPN πίσω στο εταιρικό δίκτυο, για να προσφέρει ένα ορισμένο επίπεδο ασφάλειας· ωστόσο, αν χρησιμοποιείται ένα τέτοιο μέτρο, ο εργοδότης θα πρέπει να λαμβάνει επίσης υπόψη ότι λογισμικό που εγκαθίσταται για σκοπούς παρακολούθησης παρουσιάζει κίνδυνο για την ιδιωτικότητα κατά τα διαστήματα προσωπικής χρήσης από τον εργαζόμενο. Θα μπορούσαν να χρησιμοποιηθούν συσκευές που

προσφέρουν επιπλέον προστασία, όπως περιβάλλον προστατευμένης εκτέλεσης (sandboxing) (περιορισμός των δεδομένων εντός συγκεκριμένης εφαρμογής).

Από την άλλη, ο εργοδότης πρέπει επίσης να εξετάσει το ενδεχόμενο απαγόρευσης της ιδιωτικής χρήσης ορισμένων επαγγελματικών συσκευών αν δεν υπάρχει τρόπος να αποτραπεί η παρακολούθησή της – για παράδειγμα, αν η συσκευή παρέχει τη δυνατότητα απομακρυσμένης πρόσβασης σε δεδομένα για τα οποία ο εργοδότης είναι ο υπεύθυνος επεξεργασίας.

5.4.3 *ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ (MDM)*

Η διαχείριση κινητών συσκευών δίνει τη δυνατότητα στους εργοδότες να εντοπίζουν συσκευές από απόσταση, να εφαρμόζουν συγκεκριμένες ρυθμίσεις και/ή εφαρμογές και να διαγράφουν δεδομένα κατ' απαίτηση. Ο εργοδότης ενδέχεται να χειρίζεται την εν λόγω λειτουργική δυνατότητα ο ίδιος, ή να χρησιμοποιεί για τον σκοπό αυτόν κάποιο τρίτο μέρος. Οι υπηρεσίες διαχείρισης κινητών συσκευών δίνουν επίσης στους εργοδότες τη δυνατότητα να καταγράφουν ή να παρακολουθούν τη συσκευή σε πραγματικό χρόνο, ακόμα και αν δεν έχει υποβληθεί αναφορά κλοπής της.

Θα πρέπει να διενεργείται ΕΕΠΔ πριν από τη χρήση τεχνολογίας τέτοιου είδους, όταν η τεχνολογία είναι καινούρια ή νέα για τον υπεύθυνο επεξεργασίας. Αν το συμπέρασμα της ΕΕΠΔ είναι ότι η τεχνολογία διαχείρισης κινητών συσκευών είναι απαραίτητη σε ορισμένες περιπτώσεις, θα πρέπει παρ' όλ' αυτά να διενεργηθεί εκτίμηση του αν η επεξεργασία δεδομένων που ακολουθεί συμμορφώνεται με τις αρχές της αναλογικότητας και της επικουρικότητας. Οι εργοδότες πρέπει να εξασφαλίζουν ότι τα δεδομένα που συλλέγονται στο πλαίσιο αυτής της απομακρυσμένης δυνατότητας υφίστανται επεξεργασία για συγκεκριμένο σκοπό και δεν αποτελούν, ούτε μπορούν να αποτελέσουν, μέρος ευρύτερου προγράμματος που επιτρέπει τη διαρκή παρακολούθηση των εργαζομένων. Ακόμα και στην περίπτωση ειδικών σκοπών, οι δυνατότητες παρακολούθησης θα πρέπει να μετριάζονται. Τα συστήματα παρακολούθησης μπορούν να σχεδιαστούν με τρόπο τέτοιο ώστε να καταγράφονται τα δεδομένα θέσης χωρίς να διατίθενται στον εργοδότη – στις περιπτώσεις αυτές, τα δεδομένα θέσης θα πρέπει να είναι διαθέσιμα μόνο σε περιπτώσεις όπου αναφέρεται κλοπή ή απώλεια της συσκευής.

Εργαζόμενοι των οποίων οι συσκευές είναι καταχωρισμένες σε υπηρεσίες διαχείρισης κινητών συσκευών πρέπει επίσης να ενημερώνονται πλήρως ως προς το είδος της παρακολούθησης που πραγματοποιείται και τις συνέπειες που έχει για τους ίδιους.

5.4.4 *ΦΟΡΕΤΕΣ ΣΥΣΚΕΥΕΣ*

Οι εργοδότες εξετάζουν με ολοένα και αυξανόμενη συχνότητα το ενδεχόμενο να παρέχουν στους εργαζομένους τους φορετές συσκευές, για να εντοπίζουν και να παρακολουθούν την υγεία τους και τη δραστηριότητά τους εντός, και μερικές φορές εκτός, του χώρου εργασίας. Ωστόσο, αυτή η επεξεργασία δεδομένων συνεπάγεται την επεξεργασία δεδομένων υγείας και ως εκ τούτου απαγορεύεται βάσει του άρθρου 8 της ΟΠΔ.

Δεδομένης της άνισης σχέσης μεταξύ εργοδοτών και εργαζομένων –δηλαδή του ότι ο εργαζόμενος βρίσκεται σε οικονομική εξάρτηση από τον εργοδότη– και της ευαίσθητης φύσης των δεδομένων υγείας, είναι μάλλον απίθανο να μπορεί να δοθεί νομικά έγκυρη ρητή συγκατάθεση για τον εντοπισμό ή την παρακολούθηση των δεδομένων αυτών, καθώς οι εργαζόμενοι ουσιαστικά δεν είναι εξαρχής «ελεύθεροι» να δώσουν τη συγκατάθεση αυτή.

Ακόμα και αν ο εργοδότης χρησιμοποιούσε τρίτους για τη συλλογή των δεδομένων υγείας, που θα παρείχαν στον εργοδότη μόνο συγκεντρωτικές πληροφορίες σχετικά με τις γενικές εξελίξεις υγείας, η επεξεργασία θα εξακολουθούσε να είναι παράνομη.

Επίσης, όπως περιγράφεται στη *Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης*[18], είναι τεχνικά πολύ δύσκολο να διασφαλιστεί η πλήρης ανωνυμοποίηση των δεδομένων. Ακόμα και σε περιβάλλον με περισσότερους από χίλιους εργαζομένους, δεδομένης της διαθεσιμότητας άλλων στοιχείων για τους εργαζόμενους, ο εργοδότης θα εξακολουθούσε να έχει τη δυνατότητα να ξεχωρίσει μεμονωμένους εργαζόμενους με συγκεκριμένες ενδείξεις υγείας, όπως υψηλή αρτηριακή πίεση ή παχυσαρκία.

Παράδειγμα:

Μια εταιρεία προσφέρει γενικά ως δώρο στους εργαζομένους της συσκευές παρακολούθησης της ευεξίας. Οι συσκευές μετρούν τον αριθμό βημάτων που κάνουν οι εργαζόμενοι και καταγράφουν τους καρδιακούς παλμούς και τις συνήθειές τους στον ύπνο σε βάθος χρόνου.

Τα δεδομένα υγείας που προκύπτουν θα πρέπει να είναι προσπελάσιμα μόνο από τον εργαζόμενο και όχι από τον εργοδότη. Δεδομένα που διαβιβάζονται μεταξύ εργαζομένου (ως υποκειμένου των δεδομένων) και της συσκευής / του παρόχου υπηρεσιών (ως υπεύθυνου επεξεργασίας) είναι κάτι που αφορά μόνο τα εν λόγω μέρη.

Καθώς τα δεδομένα υγείας μπορούν επίσης να υποβληθούν σε επεξεργασία από την εταιρεία που κατασκεύασε τις συσκευές ή που προσφέρει μια υπηρεσία στους εργοδότες, κατά την επιλογή της συσκευής ή της υπηρεσίας, ο εργοδότης θα πρέπει να αξιολογεί την πολιτική απορρήτου του κατασκευαστή και/ή του παρόχου υπηρεσιών ώστε να διασφαλίζει ότι δεν θα έχει ως αποτέλεσμα την παράνομη επεξεργασία των δεδομένων υγείας των εργαζομένων.

5.5 Επεξεργασία που σχετίζεται με τον χρόνο και την παρουσία

Συστήματα που παρέχουν στους εργοδότες τη δυνατότητα να ελέγχουν ποιος μπορεί να μπαίνει στις εγκαταστάσεις τους και/ή σε ορισμένους χώρους εντός των εγκαταστάσεών τους μπορούν επίσης να επιτρέψουν την παρακολούθηση των δραστηριοτήτων των εργαζομένων. Παρόλο που τέτοια συστήματα υπάρχουν εδώ και πολλά χρόνια, νέες τεχνολογίες που αποσκοπούν στην παρακολούθηση του χρόνου και της παρουσίας των εργαζομένων έχουν αρχίσει να χρησιμοποιούνται ευρύτερα· σε αυτές συγκαταλέγονται τεχνολογίες που επεξεργάζονται βιομετρικά δεδομένα, καθώς και τεχνολογίες εντοπισμού κινητών συσκευών.

Παρόλο που τα συστήματα αυτά μπορούν να αποτελέσουν σημαντικό στοιχείο για τη διαδρομή ελέγχου του εργοδότη, παρουσιάζουν επίσης τον κίνδυνο της παροχής παρεμβατικού επιπέδου γνώσης και ελέγχου ως προς τις δραστηριότητες του εργαζόμενου ενώ βρίσκεται στον χώρο εργασίας.

Παράδειγμα:

Εργοδότης διατηρεί αίθουσα διακομιστή όπου αποθηκεύονται σε ψηφιακή μορφή ευαίσθητα δεδομένα για την επιχείρηση, δεδομένα προσωπικού χαρακτήρα που αφορούν τους εργαζόμενους και δεδομένα προσωπικού χαρακτήρα που αφορούν τους πελάτες.

[18] ΟΕ29, *Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης, WP 216*, 10 Απριλίου 2014, σύνδεσμος: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_el.pdf

Προκειμένου να συμμορφωθεί με τις εκ του νόμου υποχρεώσεις του για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, ο εργοδότης έχει εγκαταστήσει σύστημα ελέγχου της πρόσβασης που καταγράφει την είσοδο και την έξοδο των εργαζομένων που διαθέτουν την κατάλληλη άδεια να εισέλθουν στην αίθουσα. Αν χαθεί οποιοδήποτε στοιχείο εξοπλισμού ή αν σημειωθεί μη εξουσιοδοτημένη πρόσβαση, απώλεια ή κλοπή δεδομένων, τα αρχεία που τηρούνται από τον εργοδότη του επιτρέπουν να προσδιορίσει ποιος είχε πρόσβαση στην αίθουσα κατά τη δεδομένη χρονική στιγμή.

Δεδομένου ότι η επεξεργασία είναι αναγκαία και δεν υποσκελίζει το δικαίωμα των εργαζομένων στην ιδιωτική ζωή, μπορεί να αποτελέσει έννομο συμφέρον σύμφωνα με το άρθρο 7 στοιχείο στ), αν οι εργαζόμενοι έχουν λάβει κατάλληλη πληροφόρηση για την επεξεργασία. Ωστόσο, η συνεχής παρακολούθηση της συχνότητας και του ακριβούς χρόνου εισόδου και εξόδου των εργαζομένων δεν μπορεί να δικαιολογηθεί αν αυτά τα δεδομένα χρησιμοποιούνται και για άλλο σκοπό, όπως η αξιολόγηση της απόδοσης των εργαζομένων.

5.6 Επεξεργασία με τη χρήση συστημάτων βιντεοπαρακολούθησης

Η βιντεοπαρακολούθηση και βιντεοεπιτήρηση συνεχίζει να παρουσιάζει παρόμοια ζητήματα για την ιδιωτικότητα των εργαζομένων όπως και πριν: τη δυνατότητα συνεχούς καταγραφής της συμπεριφοράς του εργαζομένου[19]. Οι πιο σημαντικές αλλαγές που αφορούν τη χρήση της εν λόγω τεχνολογίας στο εργασιακό πλαίσιο είναι η δυνατότητα εύκολης απομακρυσμένης πρόσβασης στα συλλεγόμενα δεδομένα (π.χ. μέσω έξυπνου τηλεφώνου)· η μείωση του μεγέθους των καμερών (μαζί με την αύξηση των δυνατοτήτων τους, π.χ. υψηλή ευκρίνεια)· και η επεξεργασία μπορεί να πραγματοποιηθεί με αυτόματη ανάλυση του περιεχομένου των βίντεο (video analytics).

Με τις δυνατότητες που δίνει η αυτόματη ανάλυση του περιεχομένου βίντεο, είναι δυνατόν για έναν εργοδότη να παρακολουθεί τις εκφράσεις του προσώπου του εργαζομένου με αυτοματοποιημένα μέσα, με σκοπό τον εντοπισμό αποκλίσεων από τα προκαθορισμένα πρότυπα κίνησης (π.χ. εργοστασιακό πλαίσιο), και ακόμα περισσότερα. Αυτό θα ήταν δυσανάλογο σε σχέση με τα δικαιώματα και τις ελευθερίες των εργαζομένων και, ως εκ τούτου, γενικά παράνομο. Η επεξεργασία είναι επίσης πιθανό να περιλαμβάνει την κατάρτιση προφίλ και, ενδεχομένως, την αυτοματοποιημένη λήψη αποφάσεων. Ως εκ τούτου, οι εργοδότες θα πρέπει να αποφεύγουν τη χρήση τεχνολογιών αναγνώρισης προσώπου. Ο κανόνας αυτός ενδέχεται να έχει κάποιες περιορισμένες εξαιρέσεις, τα σενάρια αυτά όμως δεν μπορούν να χρησιμοποιηθούν προκειμένου να γίνεται επίκληση μιας γενικής νομιμοποίησης της χρήσης της εν λόγω τεχνολογίας[20].

5.7 Επεξεργασία που αφορά οχήματα τα οποία χρησιμοποιούν οι εργαζόμενοι

Τεχνολογίες που παρέχουν στους εργοδότες τη δυνατότητα να παρακολουθούν τα οχήματά τους χρησιμοποιούνται ευρέως, ιδίως από εταιρείες οι δραστηριότητες των οποίων σχετίζονται με τις μεταφορές ή οι οποίες έχουν μεγάλους στόλους οχημάτων.

[19] Βλ. την προαναφερθείσα υπόθεση *Köpke κατά Γερμανίας*· επιπλέον, θα πρέπει να σημειωθεί ότι σε ορισμένες έννομες τάξεις, η εγκατάσταση συστημάτων όπως τηλεόραση κλειστού κυκλώματος με σκοπό την τεκμηρίωση παράνομης συμπεριφοράς έχει κριθεί επιτρεπτή· βλ. υπόθεση *Bershka* ενώπιον του Συνταγματικού Δικαστηρίου της Ισπανίας.

[20] Επιπλέον, σύμφωνα με τον ΓΚΠΔ, η επεξεργασία βιομετρικών δεδομένων για σκοπούς ταυτοποίησης πρέπει να βασίζεται σε εξαίρεση που προβλέπεται από το άρθρο 9 παράγραφος 2.

Εργοδότης που χρησιμοποιεί τηλεματική οχημάτων συλλέγει δεδομένα τόσο για το όχημα όσο και για τον συγκεκριμένο εργαζόμενο που το χρησιμοποιεί. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν όχι μόνο τη θέση του οχήματος (και, ως εκ τούτου, του εργαζόμενου) που συλλέγονται από βασικά συστήματα εντοπισμού με GPS, αλλά, ανάλογα με την τεχνολογία, μεγάλη γκάμα άλλων πληροφοριών, συμπεριλαμβανομένης της οδηγικής συμπεριφοράς. Ορισμένες τεχνολογίες μπορεί επίσης να δίνουν τη δυνατότητα της συνεχούς παρακολούθησης τόσο του οχήματος όσο και του οδηγού (π.χ. καταγραφείς δεδομένων συμβάντων).

Ο εργοδότης μπορεί να είναι υποχρεωμένος να εγκαταστήσει τεχνολογία εντοπισμού στα οχήματά του ώστε να αποδείξει τη συμμόρφωσή του με άλλες εκ του νόμου υποχρεώσεις, π.χ. τη διασφάλιση της ασφάλειας των εργαζομένων που οδηγούν αυτά τα οχήματα. Μπορεί επίσης να έχει έννομο συμφέρον να είναι σε θέση να εντοπίζει τα οχήματα ανά πάσα στιγμή. Ακόμη και αν οι εργοδότες έχουν έννομο συμφέρον για την επίτευξη των εν λόγω σκοπών, θα πρέπει πρώτα να αξιολογείται κατά πόσον η επεξεργασία είναι αναγκαία για τους σκοπούς αυτούς και αν η πραγματική εφαρμογή είναι σύμφωνη με τις αρχές της αναλογικότητας και της επικουρικότητας. Όταν επιτρέπεται η ιδιωτική χρήση επαγγελματικού οχήματος, το πιο σημαντικό μέτρο που μπορεί να λάβει ο εργοδότης για να διασφαλίσει τη συμμόρφωση με τις αρχές αυτές είναι η παροχή της δυνατότητας απενεργοποίησης: ο εργαζόμενος θα πρέπει να έχει καταρχήν τη δυνατότητα να απενεργοποιεί προσωρινά τον εντοπισμό θέσης όταν ειδικές περιστάσεις δικαιολογούν την απενεργοποίηση, όπως επίσκεψη σε γιατρό. Με τον τρόπο αυτό, ο εργαζόμενος μπορεί, με δική του πρωτοβουλία, να προστατεύει ορισμένα δεδομένα θέσης ως ιδιωτικά. Ο εργοδότης πρέπει να διασφαλίζει ότι τα συλλεγόμενα δεδομένα δεν χρησιμοποιούνται για περαιτέρω επεξεργασία, όπως η παρακολούθηση και αξιολόγηση των εργαζομένων.

Επίσης, ο εργοδότης πρέπει να ενημερώνει με σαφήνεια τους εργαζομένους ότι έχει εγκατασταθεί συσκευή παρακολούθησης σε εταιρικό όχημα το οποίο οδηγούν και ότι οι μετακινήσεις τους καταγράφονται ενώ χρησιμοποιούν το εν λόγω όχημα (και ότι, ανάλογα με τη χρησιμοποιούμενη τεχνολογία, μπορεί επίσης να καταγράφεται η οδηγική συμπεριφορά τους). Κατά προτίμηση, οι πληροφορίες αυτές θα πρέπει να είναι αναρτημένες ευκρινώς σε κάθε όχημα, εντός του οπτικού πεδίου του οδηγού.

Οι εργαζόμενοι ενδέχεται να χρησιμοποιούν τα εταιρικά οχήματα εκτός του ωραρίου εργασίας, π.χ. για προσωπική χρήση, ανάλογα με τις συγκεκριμένες πολιτικές που διέπουν τη χρήση των εν λόγω οχημάτων. Λόγω του ευαίσθητου χαρακτήρα των δεδομένων θέσης, δεν είναι πιθανό να υπάρχει νομική βάση για την παρακολούθηση της θέσης των οχημάτων των εργαζομένων εκτός του συμφωνημένου ωραρίου εργασίας. Ωστόσο, εάν υπάρχει τέτοια ανάγκη, θα πρέπει να εξετάζεται χρήση που θα είναι ανάλογη των κινδύνων. Για παράδειγμα, αυτό θα μπορούσε να σημαίνει ότι, για την πρόληψη της κλοπής οχημάτων, η θέση του οχήματος δεν καταγράφεται εκτός του ωραρίου εργασίας, εκτός εάν το όχημα εγκαταλείψει μια ευρύτερη τοποθεσία (περιφέρεια ή ακόμα και χώρα). Επιπλέον, η τοποθεσία θα εμφανίζεται μόνο σε περιπτώσεις έκτακτης ανάγκης – ο εργοδότης ενεργοποιεί την ορατότητα της θέσης, προσπελάζοντας δεδομένα που έχουν ήδη αποθηκευτεί από το σύστημα, όταν το όχημα βγαίνει από μια προκαθορισμένη περιοχή.

Όπως αναφέρεται στη *Γνώμη 13/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών* της ΟΕ29[21]:

> «Οι συσκευές εντοπισμού της θέσης οχημάτων δεν λειτουργούν ως συσκευές παρακολούθησης του προσωπικού. Σκοπός τους είναι να εντοπίζουν ή να παρακολουθούν τη θέση των οχημάτων στα οποία είναι εγκατεστημένες. Οι εργοδότες δεν θα πρέπει να χρησιμοποιούν τις συσκευές για τον εντοπισμό ή την παρακολούθηση της συμπεριφοράς ή της θέσης οδηγών ή άλλων μελών του προσωπικού, με τη χρήση για παράδειγμα της δυνατότητας αποστολής ειδοποιήσεων σε περίπτωση ανάπτυξης υπερβολικής ταχύτητας.»

Περαιτέρω, όπως ορίζεται στη *Γνώμη για τη χρήση δεδομένων θέσης με σκοπό την παροχή υπηρεσιών με προστιθέμενη αξία* της ΟΕ29[22]:

> «Η επεξεργασία δεδομένων θέσης μπορεί να δικαιολογηθεί όταν πραγματοποιείται στο πλαίσιο της παρακολούθησης της μεταφοράς ατόμων ή αγαθών ή της βελτίωσης της διανομής πόρων για υπηρεσίες σε διασκορπισμένες περιοχές (π.χ. σχεδιασμός επιχειρήσεων σε πραγματικό χρόνο), ή όταν επιδιώκεται ένας στόχος που αφορά την ασφάλεια του ίδιου του εργαζόμενου ή των εμπορευμάτων ή των οχημάτων που του έχουν ανατεθεί. Αντιθέτως, η ομάδα εργασίας κρίνει την επεξεργασία δεδομένων υπέρμετρη όταν οι εργαζόμενοι είναι ελεύθεροι να οργανώσουν τις λεπτομέρειες του ταξιδιού τους όπως επιθυμούν ή όταν αυτή πραγματοποιείται με αποκλειστικό σκοπό την παρακολούθηση της εργασίας του εργαζόμενου, εφόσον αυτή μπορεί να παρακολουθείται με άλλα μέσα.»

5.7.1 ΚΑΤΑΓΡΑΦΕΙΣ ΔΕΔΟΜΕΝΩΝ ΣΥΜΒΑΝΤΩΝ

Οι καταγραφείς δεδομένων συμβάντων παρέχουν στον εργοδότη την τεχνική δυνατότητα επεξεργασίας σημαντικού αριθμού δεδομένων προσωπικού χαρακτήρα σχετικά με τους εργαζομένους που οδηγούν εταιρικά οχήματα. Οι συσκευές αυτές τοποθετούνται με ολοένα και μεγαλύτερη συχνότητα σε οχήματα με σκοπό την καταγραφή βίντεο, ενδεχομένως και ήχου, σε περίπτωση ατυχήματος. Τα συστήματα αυτά μπορούν να διενεργούν καταγραφή σε συγκεκριμένο χρόνο, π.χ. ανταποκρινόμενα σε ξαφνικό φρενάρισμα, απότομη μεταβολή της κατεύθυνσης ή ατυχήματα, περιπτώσεις στις οποίες αποθηκεύονται και οι αμέσως προηγούμενες στιγμές του συμβάντος, μπορούν όμως να ρυθμιστούν ώστε να πραγματοποιούν συνεχή παρακολούθηση. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν στη συνέχεια για την παρατήρηση και τον έλεγχο της οδηγικής συμπεριφοράς ενός ατόμου με σκοπό τη βελτίωσή της. Επιπλέον, πολλά από τα συστήματα αυτά περιλαμβάνουν GPS για τον εντοπισμό της θέσης του οχήματος σε πραγματικό χρόνο και άλλες λεπτομέρειες που αφορούν την οδήγηση (όπως η ταχύτητα του οχήματος) μπορούν επίσης να αποθηκεύονται για περαιτέρω επεξεργασία.

Οι συσκευές αυτές έχουν καταστεί ιδιαίτερα διαδεδομένες σε εταιρείες οι δραστηριότητες των οποίων σχετίζονται με τις μεταφορές ή οι οποίες έχουν μεγάλους στόλους οχημάτων. Ωστόσο, η χρήση καταγραφέων δεδομένων συμβάντων μπορεί να είναι νόμιμη μόνο αν η επεξεργασία των προκυπτόντων δεδομένων προσωπικού χαρακτήρα του εργαζομένου είναι

[21] ΟΕ29, *Γνώμη 13/2011 σχετικά με τις υπηρεσίες εντοπισμού γεωγραφικής θέσης που παρέχονται μέσω έξυπνων κινητών συσκευών*, WP 185, 16 Μαΐου 2011, σύνδεσμος: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_el.pdf

[22] ΟΕ29, *Γνώμη 5/2005 για τη χρήση δεδομένων θέσης με σκοπό την παροχή υπηρεσιών προστιθέμενης αξίας*, WP 115, 25 Νοεμβρίου 2005, σύνδεσμος: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_el.pdf

απαραίτητη για νόμιμο σκοπό και σύμφωνη με τις αρχές της αναλογικότητας και της επικουρικότητας.

Παράδειγμα

Εταιρεία μεταφορών εξοπλίζει όλα τα οχήματά της με βιντεοκάμερα στο εσωτερικό της καμπίνας, που καταγράφει ήχο και εικόνα. Ο σκοπός της επεξεργασίας των δεδομένων αυτών είναι να βελτιωθούν οι οδηγικές ικανότητες των εργαζομένων. Οι κάμερες είναι ρυθμισμένες να διατηρούν καταγραφές όταν λαμβάνουν χώρα περιστατικά όπως ξαφνικό φρενάρισμα ή απότομη αλλαγή κατεύθυνσης. Η εταιρεία υποθέτει ότι έχει νομική βάση για την επεξεργασία η οποία συνίσταται στο έννομο συμφέρον της, σύμφωνα με το άρθρο 7 στοιχείο στ) της ΟΠΔ, να προστατεύει την ασφάλεια των εργαζομένων της και των υπολοίπων οδηγών.

Ωστόσο, το έννομο συμφέρον της εταιρείας να παρακολουθεί τους οδηγούς δεν υπερισχύει των δικαιωμάτων των εν λόγω οδηγών στην προστασία των προσωπικών τους δεδομένων. Η συνεχής παρακολούθηση των εργαζομένων με τέτοιες κάμερες αποτελεί σοβαρή παρέμβαση στο δικαίωμά τους στην ιδιωτικότητα. Υπάρχουν και άλλες μέθοδοι (π.χ. η εγκατάσταση εξοπλισμού που εμποδίζει τη χρήση κινητών τηλεφώνων), καθώς και άλλα συστήματα όπως το προηγμένο σύστημα πέδησης έκτακτης ανάγκης ή σύστημα προειδοποίησης εκτροπής από τη λωρίδα κυκλοφορίας, τα οποία μπορούν να χρησιμοποιηθούν για την πρόληψη των ατυχημάτων, τα οποία ενδέχεται να είναι καταλληλότερα. Επιπλέον, ένα τέτοιο βίντεο είναι πολύ πιθανόν να έχει ως αποτέλεσμα την επεξεργασία δεδομένων προσωπικού χαρακτήρα τρίτων (όπως οι πεζοί) και το έννομο συμφέρον της επιχείρησης δεν αρκεί για να δικαιολογήσει μια τέτοια επεξεργασία.

5.8 Επεξεργασία που αφορά την κοινολόγηση δεδομένων εργαζομένων σε τρίτους

Είναι ολοένα και συνηθέστερο να διαβιβάζουν οι εταιρείες δεδομένα των εργαζομένων τους στους πελάτες τους με σκοπό τη διασφάλιση της αξιόπιστης παροχής υπηρεσιών. Τα δεδομένα αυτά μπορεί να είναι αρκετά εκτενή, ανάλογα με την έκταση των παρεχόμενων υπηρεσιών (π.χ. μπορεί να περιλαμβάνεται σε αυτά φωτογραφία του εργαζόμενου). Ωστόσο, λόγω της ανισορροπίας της ισχύος, οι εργαζόμενοι δεν είναι σε θέση να δώσουν ελεύθερη συγκατάθεση στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα τους από τον εργοδότη τους και αν η επεξεργασία των δεδομένων δεν είναι αναλογική, ο εργοδότης δεν έχει νομική βάση.

Παράδειγμα:

Μια εταιρεία ταχυδρομικών αποστολών στέλνει στους πελάτες ηλεκτρονικό μήνυμα με σύνδεσμο που περιέχει το όνομα και την τοποθεσία του παραδίδοντος (εργαζόμενος). Η εταιρεία σκόπευε επίσης να παράσχει φωτογραφία ταυτότητας του παραδίδοντος. Η εταιρεία υπέθεσε ότι είχε νομική βάση για την επεξεργασία η οποία συνίστατο στο έννομο συμφέρον της [άρθρο 7 στοιχείο στ), της οδηγίας], ώστε να επιτρέπει στον καταναλωτή να ελέγχει εάν ο παραδίδων ήταν πράγματι το σωστό πρόσωπο.

Ωστόσο, δεν είναι απαραίτητο να παρέχονται στους πελάτες το όνομα και η φωτογραφία του παραδίδοντος. Εφόσον δεν υπάρχει άλλη νόμιμη βάση για την επεξεργασία αυτή, δεν επιτρέπεται στην εταιρεία να παρέχει τα εν λόγω δεδομένα προσωπικού χαρακτήρα στους πελάτες της.

5.9 Επεξεργασία που αφορά διεθνείς διαβιβάσεις δεδομένων ανθρωπίνων πόρων και άλλων δεδομένων των εργαζομένων

Οι εργοδότες χρησιμοποιούν όλο και συχνότερα εφαρμογές και υπηρεσίες υπολογιστικού νέφους, όπως εκείνες που είναι σχεδιασμένες για τον χειρισμό των δεδομένων ανθρωπίνων πόρων, καθώς και διαδικτυακές εφαρμογές γραφείου. Η χρήση των περισσότερων από αυτές τις εφαρμογές θα έχει ως αποτέλεσμα τη διεθνή διαβίβαση δεδομένων από και αναφορικά με τους εργαζομένους. Όπως έχει αναφερθεί στη γνώμη 8/2001, το άρθρο 25 της ΟΠΔ ορίζει ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα εκτός της ΕΕ επιτρέπεται μόνο αν η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Ανεξαρτήτως της βάσης, η διαβίβαση θα πρέπει να πληροί τις διατάξεις της οδηγίας.

Επομένως, θα πρέπει να διασφαλίζεται ότι τηρούνται οι διατάξεις αυτές που αφορούν τη διεθνή διαβίβαση δεδομένων. Η ΟΕ29 επαναλαμβάνει την προηγούμενη θέση της, ότι είναι προτιμότερο να γίνεται επίκληση της επαρκούς προστασίας και όχι των παρεκκλίσεων που απαριθμούνται στο άρθρο 26 της ΟΠΔ· όταν γίνεται επίκληση της συγκατάθεσης, αυτή πρέπει να είναι ρητή, σαφής και ελεύθερη. Ωστόσο, θα πρέπει επίσης να διασφαλίζεται ότι τα δεδομένα που διαβιβάζονται εκτός της ΕΕ/του ΕΟΧ και η μετέπειτα πρόσβαση από άλλες οντότητες του ομίλου εξακολουθούν να περιορίζονται στο ελάχιστο αναγκαίο για τους επιδιωκόμενους σκοπούς.

6. Συμπεράσματα και συστάσεις

6.1 Θεμελιώδη δικαιώματα

Το περιεχόμενο των προαναφερθεισών επικοινωνιών, καθώς και των δεδομένων κυκλοφορίας που σχετίζονται με τις επικοινωνίες, απολαμβάνουν τα ίδια θεμελιώδη δικαιώματα όπως και οι αναλογικές επικοινωνίες.

Οι ηλεκτρονικές επικοινωνίες που πραγματοποιούνται από εμπορικές εγκαταστάσεις ενδέχεται να καλύπτονται από τις έννοιες της «ιδιωτικής ζωής» και της «αλληλογραφίας» κατά την έννοια του άρθρου 8 παράγραφος 1 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου. Βάσει της ισχύουσας οδηγίας για την προστασία των δεδομένων, οι εργοδότες μπορούν να συλλέγουν δεδομένα μόνο για νόμιμους σκοπούς, η επεξεργασία πρέπει να πραγματοποιείται σύμφωνα με τις κατάλληλες προϋποθέσεις (π.χ. να είναι αναλογική και αναγκαία, να ανταποκρίνεται σε πραγματικό και υφιστάμενο συμφέρον, να γίνεται με νόμιμο, δηλωμένο και διαφανή τρόπο) και να υφίσταται νομική βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που συλλέγονται ή παράγονται από τις ηλεκτρονικές επικοινωνίες.

Το γεγονός ότι ένας εργοδότης έχει την κυριότητα των ηλεκτρονικών μέσων δεν αποκλείει το δικαίωμα των εργαζομένων στο απόρρητο των επικοινωνιών τους, των σχετικών δεδομένων θέσης και της αλληλογραφίας τους. Η παρακολούθηση της θέσης των εργαζομένων μέσω ιδιόκτητων ή εταιρικών συσκευών θα πρέπει να περιορίζεται στον βαθμό που είναι απολύτως απαραίτητος για νόμιμο σκοπό. Βεβαίως, στην περίπτωση της χρήσης προσωπικών συσκευών, έχει σημασία να δίνεται στους εργαζόμενους η ευκαιρία να προστατεύουν τις ιδιωτικές επικοινωνίες τους από οποιαδήποτε παρακολούθηση που σχετίζεται με την εργασία.

6.2 Συγκατάθεση· έννομο συμφέρον

Οι εργαζόμενοι σπάνια είναι σε θέση να δώσουν, να αρνηθούν ή να ανακαλέσουν τη συγκατάθεσή τους, δεδομένης της εξάρτησης που προκύπτει από τη σχέση μεταξύ εργοδότη και εργαζόμενου. Δεδομένης της ανισορροπίας της ισχύος, οι εργαζόμενοι μπορούν να παρέχουν ελεύθερη συγκατάθεση μόνο σε εξαιρετικές περιστάσεις, όταν καμία απολύτως συνέπεια δεν συνδέεται με την αποδοχή ή απόρριψη της προσφοράς.

Ενίοτε, μπορεί να γίνεται επίκληση του έννομου συμφέροντος των εργοδοτών ως νομική βάση, αλλά μόνον αν η επεξεργασία είναι απολύτως αναγκαία για νόμιμο σκοπό και είναι σύμφωνη με τις αρχές της αναλογικότητας και της επικουρικότητας. Πριν από τη χρήση οποιουδήποτε εργαλείου παρακολούθησης θα πρέπει να πραγματοποιείται έλεγχος αναλογικότητας, ώστε να εξετάζεται αν όλα τα δεδομένα είναι απαραίτητα, αν η εν λόγω επεξεργασία υποσκελίζει τα γενικότερα δικαιώματα ιδιωτικότητας που οι εργαζόμενοι έχουν και στον χώρο εργασίας και ποια μέτρα πρέπει να ληφθούν για να διασφαλίζεται ότι οι παραβάσεις του δικαιώματος στην ιδιωτική ζωή και του δικαιώματος του απορρήτου των επικοινωνιών περιορίζονται στο ελάχιστο αναγκαίο.

6.3 Διαφάνεια

Θα πρέπει να παρέχεται στους εργαζομένους αποτελεσματική ενημέρωση σχετικά με τυχόν παρακολούθηση που πραγματοποιείται, με τους σκοπούς και τις συνθήκες της παρακολούθησης αυτής, καθώς και τις δυνατότητες των εργαζομένων να αποτρέπουν την καταγραφή των δεδομένων τους από τεχνολογίες παρακολούθησης. Οι πολιτικές και οι κανόνες σχετικά με την νόμιμη παρακολούθηση πρέπει να είναι σαφείς και να παρέχεται η δυνατότητα εύκολης πρόσβασης σε αυτά. Η ομάδα εργασίας συνιστά τη συμμετοχή ενός αντιπροσωπευτικού δείγματος εργαζομένων στη δημιουργία και την αξιολόγηση των εν λόγω κανόνων και πολιτικών, καθώς το μεγαλύτερο μέρος της παρακολούθησης ενδέχεται να παραβιάζει την ιδιωτική ζωή των εργαζομένων.

6.4 Αναλογικότητα και ελαχιστοποίηση των δεδομένων

Η επεξεργασία δεδομένων στην εργασία πρέπει να συνιστά αναλογική αντίδραση στους κινδύνους που αντιμετωπίζει ο εργοδότης. Για παράδειγμα, η κατάχρηση του διαδικτύου μπορεί να εντοπιστεί χωρίς να απαιτείται η ανάλυση του περιεχομένου δικτυακών τόπων. Αν μπορεί να προληφθεί η κατάχρηση (π.χ. με τη χρήση διαδικτυακών φίλτρων), ο εργοδότης δεν έχει γενικό δικαίωμα παρακολούθησης.

Επίσης, η γενική απαγόρευση της επικοινωνίας για προσωπικούς λόγους δεν είναι πρακτική και η επιβολή της μπορεί να απαιτεί ενδεχομένως δυσανάλογο επίπεδο ελέγχου. Θα πρέπει να δίνεται πολύ μεγαλύτερη βαρύτητα στην πρόληψη από ό,τι στον εντοπισμό – τα συμφέροντα του εργοδότη εξυπηρετούνται καλύτερα με την πρόληψη της κατάχρησης του διαδικτύου με τεχνικά μέσα από ό,τι με τη δαπάνη πόρων για τον εντοπισμό της κατάχρησης.

Οι πληροφορίες που καταγράφονται από τη συνεχή παρακολούθηση, καθώς και οι πληροφορίες που επιδεικνύονται στον εργοδότη, θα πρέπει να ελαχιστοποιούνται όσο το δυνατόν περισσότερο. Οι εργαζόμενοι θα πρέπει να έχουν τη δυνατότητα να απενεργοποιούν προσωρινά τον εντοπισμό θέσης, εφόσον αυτό δικαιολογείται από τις περιστάσεις. Λύσεις που συνίστανται, για παράδειγμα, στην παρακολούθηση οχημάτων, μπορούν να σχεδιαστούν με τρόπο τέτοιο ώστε να διενεργείται καταγραφή των δεδομένων θέσης, χωρίς να παρουσιάζονται στον εργοδότη.

Οι εργοδότες πρέπει να λαμβάνουν υπόψη την αρχή της ελαχιστοποίησης των δεδομένων, όταν αποφασίζουν σχετικά με τη χρήση νέων τεχνολογιών. Οι πληροφορίες θα πρέπει να αποθηκεύονται για το ελάχιστο χρονικό διάστημα που απαιτείται με καθορισμένη περίοδο διατήρησης. Πληροφορίες που δεν είναι πλέον απαραίτητες θα πρέπει να διαγράφονται.

6.5 Υπηρεσίες υπολογιστικού νέφους, διαδικτυακές εφαρμογές και διεθνείς διαβιβάσεις

Όταν οι εργαζόμενοι οφείλουν να χρησιμοποιούν διαδικτυακές εφαρμογές που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα (όπως οι διαδικτυακές εφαρμογές γραφείου), οι εργοδότες θα πρέπει να εξετάζουν το ενδεχόμενο να δίνουν στους εργαζόμενους τη δυνατότητα να ορίζουν ιδιωτικά τμήματα τα οποία ο εργοδότης δεν μπορεί να προσπελάσει σε καμία περίπτωση, όπως φάκελο ιδιωτικής αλληλογραφίας ή εγγράφων.

Η χρήση των περισσότερων εφαρμογών εντός του υπολογιστικού νέφους θα έχει ως αποτέλεσμα τη διεθνή διαβίβαση των δεδομένων των εργαζομένων. Θα πρέπει να διασφαλιστεί ότι δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα εκτός ΕΕ μόνον εφόσον εξασφαλίζεται κατάλληλο επίπεδο προστασίας και ότι τα δεδομένα που διαβιβάζονται εκτός ΕΕ/ΕΟΧ και η μετέπειτα πρόσβαση από άλλες οντότητες του ομίλου εξακολουθούν να περιορίζονται στο ελάχιστο αναγκαίο για τους επιδιωκόμενους σκοπούς.

* * *

Βρυξέλλες, 8 Ιουνίου 2017

Για την ομάδα εργασίας,
Η πρόεδρος
Isabelle FALQUE-PIERROTIN