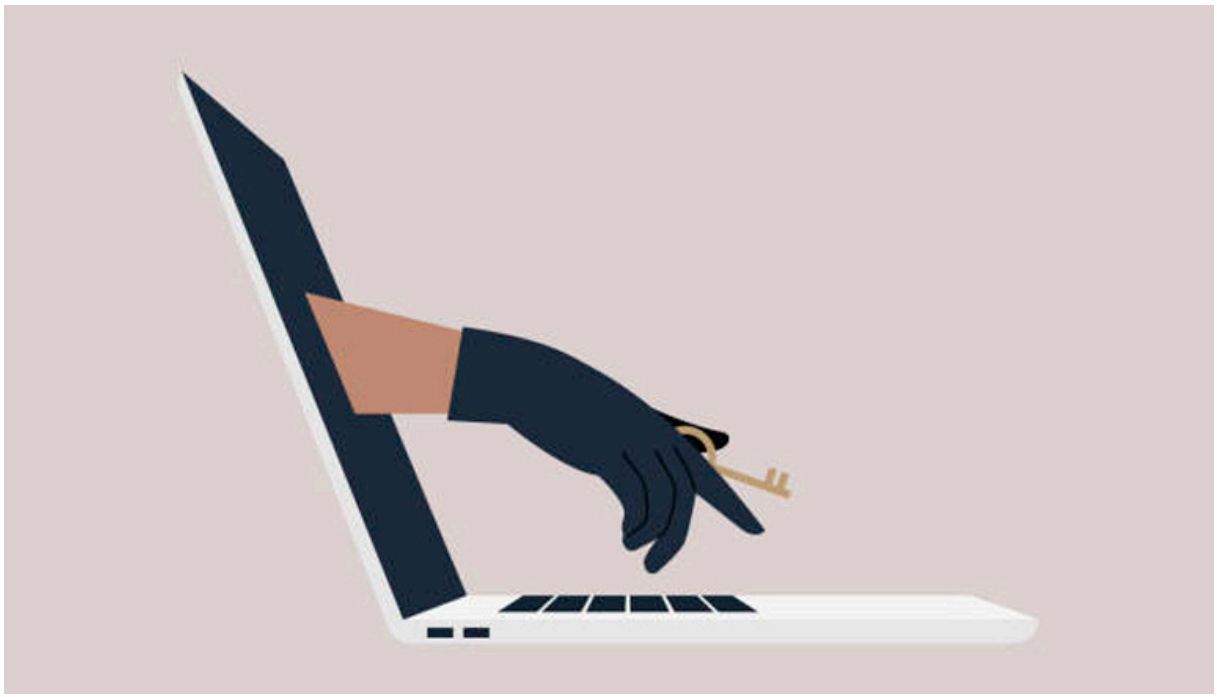
Παράνομη απόκτηση πρόσβασης σε δεδομένα από δράστη που βρίσκεται στην υπηρεσία του νόμιμου κατόχου

Νικόλας Γανιάρης
Δικηγόρος, Υπ. ΔΝ ΕΚΠΑ



Μετάφραση και παρατηρήσεις επί της υπό στοιχεία 5 StR 614/19 – 13.5.2020 αποφάσεως του γερμανικού Ακυρωτικού Δικαστηρίου, όπως δημοσιεύθηκε σε: HöchstRichterliche Rechtsprechung im Strafrecht 2020 Nr. 800

Σκεπτικό

Το Πρωτοδικείο καταδίκασε τον κατηγορούμενο Η για τα αδικήματα της κλοπής με διάρρηξη, της υποκλοπής δεδομένων σε δύο περιπτώσεις και της κατοχής υλικού παιδικής πορνογραφίας σε συνολική ποινή ενός έτους και έντεκα μηνών, την εκτέλεση της οποίας ανέστειλε υπό

όρους. Το Δικαστήριο αναγνώρισε ότι έχουν εκτιθεί πέντε μήνες από την επιβληθείσα ποινή. Επιπλέον, διέταξε εις βάρος του Η τη δήμευση των προϊόντων του εγκλήματος αξίας 70.900 ευρώ. Ο κατηγορούμενος Β καταδικάστηκε για υποκλοπή δεδομένων σε δύο περιπτώσεις σε συνολική χρηματική ποινή 300 ημερησίων μονάδων, αξίας 220 ευρώ η καθεμία, εκ των οποίων 60 ημερήσιες μονάδες έχουν αποτιθεί. […] Οι αιτήσεις αναίρεσης των κατηγορουμένων Η και Β, που βασίζονται σε νομικές και ουσιαστικές αιτιάσεις, αποσκοπούν όσον αφορά τον κατηγορούμενο Η σε μείωση του ποσού επί του οποίου επιβλήθηκε η δήμευση και όσον αφορά τον κατηγορούμενο Β σε αναίρεση της καταδικαστικής απόφασης. Κατά τα λοιπά, οι αιτήσεις αναίρεσης πρέπει να απορριφθούν ως αβάσιμες εν τη εννοία του άρθρου 349 παρ. 2 γερμΚΠΔ (βλ. την πρόταση του Γενικού Ομοσπονδιακού Εισαγγελέα).
Α) Αίτηση αναίρεσης του κατηγορουμένου Η
Η απόφαση είναι ορθή, καθ' ο μέρος το Πρωτοδικείο έκρινε τον κατηγορούμενο Η ένοχο για υποκλοπή δεδομένων[1] (άρθρο 202a γερμΠΚ) σε δύο περιπτώσεις.

I.

1. Το Πρωτοδικείο διεπίστωσε τα ακόλουθα.

Ο κατηγορούμενος Β γνώρισε τον κατηγορούμενο Η, όταν χρησιμοποίησε τις σεξουαλικές του υπηρεσίες ως «Callboy» τον Μάιο του 2006. Εν συνεχεία συναντήθηκαν περισσότερες φορές το 2007 και το 2008. Τον Ιούλιο του 2007, ο Β έγινε υπεύθυνος διεύθυνσης του λόμπι φαρμακευτικών εταιρειών Α και ενημέρωνε τον ιστότοπο διαδικτυακών πληροφοριών «a-a». Στον ιστότοπο αυτόν δημοσιεύονταν συχνά εσωτερικές πληροφορίες[2] από το Ομοσπονδιακό Υπουργείο Υγείας, οι οποίες είχαν ιδιαίτερο ενδιαφέρον για τον τομέα των φαρμακευτικών εταιρειών και των φαρμακείων. Στο Υπουργείο υπήρχαν κατά τα έτη 2006 έως 2012, όπως και παλαιότερα, διαρροές, υπό την έννοια της αθέμιτης μετάδοσης εσωτερικών πληροφοριών της διοίκησης. Τον Ιούλιο του 2008, ο κατηγορούμενος Η ορίστηκε από τον εργοδότη του «διαχειριστής συστήματος» του Υπουργείου στο γραφείο Βερολίνου.

Οι δύο κατηγορούμενοι συμφώνησαν το αργότερο τον Ιανουάριο του 2009 ότι ο Η θα προμήθευε τον Β με εσωτερικές πληροφορίες από το Υπουργείο, τις οποίες ο τελευταίος επιθυμούσε

1. Το έγκλημα του άρθρου 202a γερμΠΚ (Ausspähen von Daten) αποδίδεται στα ελληνικά ως «κατασκοπεία δεδομένων», σύμφωνα με το Ελληνο-Γερμανικό Λεξικό Νομικών Όρων (επιστ. επιμ. Βαθιώτη, 2013). Προτιμήθηκε, όμως, ο όρος «υποκλοπή δεδομένων» για να αποφευχθεί η σύγχυση με το αδίκημα της Κατασκοπείας (άρθρο 148 ΠΚ).

2. [2] Στην απόφαση χρησιμοποιείται ο όρος «Hintergrundinformationen».

να χρησιμοποιήσει για τις επαγγελματικές του δραστηριότητες. Ο κατηγορούμενος Η είχε ως διαχειριστής συστήματος τη δυνατότητα να αποκτά πρόσβαση σε όλους τους λογαριασμούς ηλεκτρονικού ταχυδρομείου και να λαμβάνει γνώση του περιεχομένου των αποθηκευμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου μετά την είσοδό του με τον κωδικό του στον κεντρικό κατάλογο του συστήματος. Γι' αυτό συχνά χρησιμοποιούσε για τη δραστηριότητά του ως διαχειριστή συστήματος το προφίλ χρήστη «P», το οποίο δημιουργήθηκε για εκπαιδευτικούς λόγους, και είχε εγγραφεί στην ομάδα χρηστών «E.D.S.». Ο κωδικός πρόσβασης του προφίλ χρήστη «P» ήταν γενικά γνωστός στους διαχειριστές του Υπουργείου.

Το Υπουργείο τροποποίησε τα δικαιώματα πρόσβασης από τις 20 Ιουλίου 2009, διότι η απεριόριστη δυνατότητα προσπέλασης των διαχειριστών σε όλους τους λογαριασμούς ηλεκτρονικού ταχυδρομείου χαρακτηρίστηκε ως έλλειμα ασφαλείας. Οι διαχειριστές δεν ήταν πλέον εγγεγραμμένοι στην ομάδα χρηστών «E.D.S.» του κεντρικού καταλόγου του συστήματος και μπορούσαν να έχουν ακώλυτη πρόσβαση μόνο στους δημόσιους λογαριασμούς ηλεκτρονικού ταχυδρομείου των τμημάτων και των τομέων. Αρχικά, οι διαχειριστές μπορούσαν να εισέρχονται στην ομάδα χρηστών «E.D.S.», παρότι τους είχε απαγορευθεί, και έτσι είχαν πρόσβαση στους προσωπικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου. Όμως και αυτή η δυνατότητα διεκόπη στις αρχές του Οκτωβρίου 2009. Έκτοτε οι διαχειριστές είχαν πρόσβαση αποκλειστικά στους δημόσιους λογαριασμούς ηλεκτρονικού ταχυδρομείου.

Εντούτοις, ανέκυψε η ανάγκη να αποκτήσουν οι διαχειριστές πρόσβαση στους προσωπικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου για τη διαπεραίωση ορισμένων καθηκόντων (όπως λ.χ. ανάκτηση διαγεγραμμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή δημιουργία νέων λογαριασμών ηλεκτρονικού ταχυδρομείου στους νέους συνεργάτες). Γι' αυτό προβλέφθηκε μια πολύπλοκη διαδικασία, κατά την οποία οι διαχειριστές θα έπρεπε να ενεργούν υπό την επίβλεψη του εκάστοτε υπαλλήλου του Υπουργείου, είτε παρουσία αυτού είτε με λειτουργία απομακρυσμένης σύνδεσης από τον χώρο εργασίας, μετά την είσοδο του υπαλλήλου στο σύστημα με τον κωδικό. Όταν η λειτουργία απομακρυσμένης σύνδεσης δεν ήταν διαθέσιμη ή όταν, όπως συνέβαινε πιο συχνά, οι συνεργάτες ζητούσαν να αντιμετωπίσουν τα προβλήματα στο μεσημεριανό διάλειμμα ή σε χρόνο απουσίας, η σύνδεση του διαχειριστή ήταν δυνατή με έναν κωδικό έκτακτης ανάγκης που δημιουργείτο κεντρικά. Η διαδικασία αυτή ήταν ιδιαίτερα χρονοβόρα. Γι' αυτό, λίγο μετά τις 20 Ιουλίου 2009, αρκετοί διαχειριστές εξέφρασαν την επιθυμία τους για μια ευκολότερη λύση.

Ο μάρτυρας P, υπεύθυνος διαχειριστής συστήματος του Υπουργείου, υπέδειξε στους διαχειριστές ότι θα μπορούσαν να αποκτήσουν πρόσβαση σε ορισμένους προσωπικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου των συνεργατών του Υπουργείου χωρίς ιδιαίτερη δυσκολία, παρα-

κάμπτοντας τους ως άνω περιορισμούς. Προς τον σκοπό αυτόν, οι διαχειριστές έπρεπε, χρησιμοποιώντας το υπηρεσιακό προφίλ του εκάστοτε χρήστη και επιλέγοντας τις ρυθμίσεις «Γενικό», «Ιδιότητες», «Αλλαγή-Διεύρυνση» και εν συνεχεία «Δικαίωμα πρόσβασης στην ηλεκτρονική θυρίδα», να εγγραφούν οι ίδιοι στη λίστα των δικαιούχων πρόσβασης, να κάνουν κλικ σε επιλογές όπως «Δικαίωμα ανάγνωσης» και «Πλήρης πρόσβαση στην ηλεκτρονική θυρίδα» και να επιβεβαιώσουν αυτές τις ρυθμίσεις με την επιλογή ΟΚ σε ένα τετραγωνίδιο. Με αυτόν τον τρόπο, μπορούσαν να προσπελάσουν το ηλεκτρονικό ταχυδρομείο του εκάστοτε συνεργάτη με το πρόγραμμα «Outlook» και είχαν τη δυνατότητα να διεκπεραιώσουν τις αναγκαίες λειτουργίες. Αυτές οι ενέργειες, που μπορούσαν να εκτελεστούν με μερικά κλικ του ποντικιού και σε ελάχιστα λεπτά, δημιούργησαν ακολούθως τη δυνατότητα για αντιγραφή του περιεχομένου ορισμένων φακέλων όπως «Ηλεκτρονική αλληλογραφία» και «Απεσταλμένα μηνύματα».

Το αργότερο από το τέλος του 2009 μέχρι τις 6 Νοεμβρίου 2012, ο κατηγορούμενος Η απέκτησε σε 33 περιπτώσεις πρόσβαση σε δημόσιους και ιδιωτικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου, τους οποίους προηγουμένως είχε υποδείξει ο κατηγορούμενος Β. Τελικά, ο Η αντέγραψε τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα αποθήκευσε σε ένα CD και τα παρέδωσε για 600 ευρώ και εν συνεχεία για 400 ευρώ στον Β ή στη συνεργάτιδά του. Ο κατηγορούμενος Η έπραξε όπως περιγράφηκε ανωτέρω, χρησιμοποιώντας δηλαδή το προφίλ χρήστη «Ρ». Μετά την αντιγραφή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, ο ίδιος αφαίρεσε το προφίλ «Ρ» από τη λίστα των δικαιούχων πρόσβασης. Ο κατηγορούμενος Β δεν γνώριζε τον τρόπο και τη μέθοδο απόκτησης πρόσβασης στα δεδομένα που ζητούσε. Θεωρούσε πιθανόν ότι ο κατηγορούμενος Η θα έπρεπε να «κάνει κάποιο κόλπο» για να αποκτήσει τα δεδομένα. Ο Β ενδιαφερόταν ιδιαιτέρως για μηνύματα ηλεκτρονικού ταχυδρομείου του εκάστοτε υπουργού, των γενικών γραμματέων και συγκεκριμένων τμηματαρχών και τομεαρχών (όπως των τμημάτων υγειονομικής περίθαλψης, ασφάλισης για ιατροφαρμακευτική περίθαλψη, ασφάλισης για χρόνια περίθαλψη, του τομέα φαρμακευτικής περίθαλψης, όπως και για θεμελιώδη ζητήματα, τον νόμο για τη λειτουργία των φαρμακείων, επαγγελματικά ζητήματα φαρμακοποιών), καθώς και της υπεύθυνης του επιτελείου του Υπουργείου. Ενημέρωσε δε τον Η γι' αυτά τα ονόματα.

Μετά την αποχή από την άσκηση ποινικής δίωξης για ορισμένες πράξεις κατά το άρθρο 154 παρ. 2 γερμΚΠΔ, αντικείμενο της δίκης είναι οι περιπτώσεις 28 και 40. Στην περίπτωση 28 ο Η, λίγες μέρες πριν από τις 10 Φεβρουαρίου του 2012 αλλά και εκείνη την ημέρα, αντέγραψε, κατόπιν απαιτήσεως του Β, πολυάριθμα μηνύματα ηλεκτρονικού ταχυδρομείου από τους ιδιωτικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου του Υπουργού Β (55 μηνύματα), του τμηματάρχη D (634 μηνύματα), της γενικής γραμματέως F (195 μηνύματα), της υπεύθυνης του επιτελείου W (699 μηνύματα), του νομικού Ο (302 μηνύματα), του τμηματάρχη Μ (184 μηνύματα), της τμηματάρχη Μ (167 μηνύματα). Εν συνεχεία, αντέγραψε τα δεδομένα σε ένα

CD και το παρέδωσε έναντι αμοιβής 600 ευρώ στον Β. Τα μηνύματα αφορούσαν ιδίως την αναθεώρηση του κανονισμού λειτουργίας φαρμακείων, το σχέδιο νόμου για τη ρύθμιση των φαρμακευτικών προϊόντων (το οποίο σχετιζόταν και με τις αμοιβές των φαρμακοποιών) και τα αποτελέσματα εμπιστευτικών διαπραγματεύσεων σχετικά με το ύψος των επιστρεπτέων εισφορών για φάρμακα με νέες δραστικές ουσίες. Στην περίπτωση 40, ο κατηγορούμενος Η αντέγραψε, λίγες μέρες πριν από τις 6 Νοεμβρίου 2012 αλλά και εκείνη την ημέρα εκ νέου, πολυάριθμα μηνύματα ηλεκτρονικού ταχυδρομείου των ως άνω προσώπων (συνολικά 2.378) που αφορούσαν το χρονικό διάστημα από τις αρχές Οκτωβρίου έως τις 5 Νοεμβρίου 2012. Τα μηνύματα αφορούσαν μεταξύ άλλων πραγματικές διαπραγματεύσεις για τις αμοιβές με την Ομοσπονδιακή Ένωση Συμβεβλημένων Ιατρών, την υποχρεωτική ασφάλιση ασθενείας ([εννοείται: με χαρακτηρισμό] «Παρακαλώ αυστηρά εμπιστευτικός χειρισμός») και την πρόταση του Υπουργού για θεσμοθέτηση κατ' αποκοπήν αμοιβής για την εφημερία και τις υπηρεσίες έκτακτων περιστατικών των φαρμακείων. Ο Η έδωσε το CD με τα δεδομένα το πρωί της 6 Νοεμβρίου 2012 στον Β έναντι αμοιβής 400 ευρώ.

Ο Β εκμεταλλευόταν τα δεδομένα που του μετέδιδε ο Η ως εσωτερικές πληροφορίες για τον διαδικτυακό του ιστότοπο «a-a». Κατ' αυτόν τον τρόπο, επεδίωκε να επιτύχει μεγάλο αριθμό επισκεπτών, ώστε να παρακινήσει τους πελάτες να καταχωρίσουν αγγελίες επί πληρωμή. Έτσι αποκτούσε ο ιστότοπος έσοδα. Ο κατηγορούμενος Η είχε δεσμευθεί από τη σύμβαση εργασίας με τον εργοδότη Β σε προστασία της εμπιστευτικότητας των δεδομένων. Η μετάδοση εσωτερικών πληροφορίων της υπηρεσίας απαγορευόταν. Δεν υφίστατο κάποια υποχρέωση έναντι του Ομοσπονδιακού Υπουργείου Υγείας από τον νόμο περί τυπικών υποχρεώσεων μη δημοσίων υπαλλήλων.[3]

2. Το Πρωτοδικείο έκρινε ότι οι δύο πράξεις που αφορούσαν τα αποθηκευμένα σε ιδιωτικούς λογαριασμούς μηνύματα ηλεκτρονικού ταχυδρομείου στοιχειοθετούσαν υποκλοπή δεδομένων από κοινού, σύμφωνα με το άρθρο 202a γερμΠΚ. Αξιολόγησε τη χειραγώγηση των δικαιωμάτων πρόσβασης επί των λογαριασμών ηλεκτρονικού ταχυδρομείου ως υπέρβαση μέτρων ασφαλείας κατά το άρθρο 202a παρ. 1 γερμΠΚ. Στην απόφαση για τη δήμευση, το Πρωτοδικείο έλαβε υπόψη και τα έσοδα του κατηγορουμένου Η από τις περιπτώσεις στις οποίες ο εισαγγελέας απείχε από την ποινική δίωξη σύμφωνα με το άρθρο 154 παρ. 2 γερμΚΠΔ.

3. Έτσι αποδίδεται στα ελληνικά ο όρος «Verpflichtungsgesetz» σύμφωνα με το Ελληνο-Γερμανικό Λεξικό Νομικών Όρων (επιστ. επιμ. Βαθιώτη, 2013).

II.

1. Η αίτηση αναίρεσης του κατηγορουμένου Η γίνεται εν μέρει δεκτή καθ' ο μέρος αφορά την απόφαση για τη δήμευση, είναι όμως κατά τα λοιπά αβάσιμη.

α) Δεν υφίστανται δικονομικά κωλύματα. Με την απαγγελία της κατηγορίας για τις πράξεις που αποτελούν αντικείμενο της δίκης σύμφωνα με το άρθρο 202a γερμΠΚ, η εισαγγελική αρχή επιβεβαίωσε, τουλάχιστον συμπερασματικά, το ιδιαίτερο δημόσιο συμφέρον για τη δίωξη των αξιόποινων πράξεων εν τη εννοία του άρθρου 205 παρ. 1 γερμΠΚ […], έτσι ώστε να μην τίθεται ζήτημα παραδεκτού της από 14 Σεπτεμβρίου 2012 εγκλήσεως.

β) Οι διαπιστώσεις [εννοείται: του Πρωτοδικείου], οι οποίες στηρίζονται σε ορθή εκτίμηση των αποδεικτικών μέσων, άγουν σε καταδίκη του κατηγορουμένου Η για υποκλοπή δεδομένων σε δύο περιπτώσεις.

Σύμφωνα με το άρθρο 202a παρ. 1 γερμΠΚ κατά την ισχύουσα από τις 11 Αυγούστου 2007 μορφή του (Εφημερίδα Ομοσπονδιακής Νομοθεσίας I 1786), είναι αξιόποινος όποιος αποκτά για τον εαυτό του ή για άλλον χωρίς δικαίωμα και διά της υπερβάσεως μέτρων προστασίας πρόσβαση σε δεδομένα τα οποία δεν προορίζονται γι' αυτόν και είναι ιδιαιτέρως προστατευμένα έναντι της μη εξουσιοδοτημένης πρόσβασης.

αα) Εφόσον ο κατηγορούμενος Η απέκτησε πρόσβαση στο περιεχόμενο των ηλεκτρονικά αποθηκευμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου από τους προσωπικούς λογαριασμούς των συνεργατών στο Υπουργείο και αντέγραψε τα δεδομένα αυτά, ο ίδιος δεν απέκτησε απλά πρόσβαση στα δεδομένα, αλλά [εννοείται: απέκτησε] τα δεδομένα καθ' εαυτά. Το γεγονός ότι τα δεδομένα δεν προορίζονταν για τον κατηγορούμενο προκύπτει από τα περιορισμένα δικαιώματα πρόσβασης που είχε ως διαχειριστής. Σε αυτά δεν περιλαμβάνονταν η ανάγνωση και αντιγραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου που δεν σχετίζονταν με τα καθήκοντά του από τους προσωπικούς λογαριασμούς των συνεργατών του. Τα δικαιώματα πρόσβασης του κατηγορουμένου περιορίζονταν αποκλειστικά σε τεχνικές εργασίες για τη διαχείριση του δικτύου.

ββ) Αυτά τα δεδομένα ήταν ιδιαιτέρως προστατευμένα έναντι μη εξουσιοδοτημένης πρόσβασης.

1) Τούτο συμβαίνει όταν υφίστανται μέτρα που αποκλείουν ή τουλάχιστον δυσχεραίνουν σημαντικά την πρόσβαση στα δεδομένα. Μέσω των μέτρων προστασίας, πρέπει ο δικαιούχος να δείξει το έννομο συμφέρον του για τη διατήρηση της εμπιστευτικότητας [εννοείται: των δεδομένων] […].

2) Εν προκειμένω, η πρόσβαση στο σύστημα ηλεκτρονικής επεξεργασίας του εκάστοτε συνεργάτη και στον προσωπικό του λογαριασμό ηλεκτρονικού ταχυδρομείου προστατευόταν, όπως συνηθίζεται, με κωδικό […]. Αυτό αρκεί προκειμένου να θεωρηθεί ότι υφίσταται μέτρο προστασίας […].

Η ύπαρξη μέτρου προστασίας πρέπει να κριθεί με βάση τη γενικότερη ασφάλεια των δεδομένων έναντι της μη εξουσιοδοτημένης πρόσβασης και όχι με βάση το γεγονός ότι ειδικοί ή μυημένοι θα μπορούσαν εύκολα να αποκτήσουν πρόσβαση στα δεδομένα […]. Δεν απαιτείται το μέτρο προστασίας να λειτουργεί αποτελεσματικά έναντι του δράστη […]. Δεν ασκεί επιρροή ότι ο κατηγορούμενος είχε αντικειμενικά πρόσβαση επί των δεδομένων ως διαχειριστής συστήματος […].

γγ) Ο κατηγορούμενος Η απέκτησε πρόσβαση επί των δεδομένων υπερβαίνοντας αυτά τα μέτρα προστασίας.
1) Με τον όρο αυτόν, ο νομοθέτης αποκλείει από το πεδίο της αντικειμενικής υπόστασης ορισμένες περιπτώσεις στις οποίες ο δράστης αποκτά τα ιδιαιτέρως προστατευμένα δεδομένα με άλλους τρόπους. Αφενός μεν αποκλείονται από το πεδίο εφαρμογής του νόμου περιπτώσεις ήσσονος σημασίας, αφετέρου δε τίθεται με το στοιχείο της προστασίας της πρόσβασης ένα σημαντικό εμπόδιο στον δράστη, η υπέρβαση του οποίου εκδηλώνει την εγκληματική ενέργεια. Θα πρέπει να γίνει δεκτό ότι καταλαμβάνονται από τη διάταξη περιπτώσεις κατά τις οποίες ο δράστης εξαναγκάζεται σε μια μορφή πρόσβασης που ο δικαιούχος των δεδομένων θέλει καταφανώς να εμποδίσει. Αυτό όμως δεν αφορά την παραβίαση οργανωτικών μέτρων ή υποχρεώσεων καταγραφής […].

Εφόσον στα έγγραφα που συνοδεύουν τον νόμο αναφέρεται ότι η παραβίαση των μέτρων προστασίας προϋποθέτει μια όχι ασήμαντη χρονικά ή τεχνικά εργασία (γι' αυτό εξάλλου δεν πληρούται η αντικειμενική υπόσταση σε περιπτώσεις στις οποίες η παραβίαση της προστασίας είναι άνευ ετέρου δυνατή), το Δικαστήριο αντιλαμβάνεται τούτο υπό την έννοια ότι η υπέρβαση των μέτρων προστασίας της πρόσβασης προϋποθέτει κατά κανόνα, ανεξάρτητα δηλαδή από τις ιδιαίτερες δυνατότητες ή γνώσεις του συγκεκριμένου δράστη, κάποια –όχι ασήμαντη– δυσχέρεια. Ως υπέρβαση νοείται η συμπεριφορά που είναι κατάλληλη για να απενεργοποιήσει ή να παρακάμψει το μέτρο προστασίας […]. Η αντικειμενική υπόσταση πληρούται ακόμα κι αν το μέτρο προστασίας μπορεί να παρακαμφθεί γρήγορα και χωρίς ιδιαίτερη δυσχέρεια λόγω ιδιαίτερων γνώσεων, ικανοτήτων ή δυνατοτήτων [εννοείται: του συγκεκριμένου δράστη]. Για το προστατευόμενο έννομο αγαθό, ήτοι το τυπικό δικαίωμα του νόμιμου κατόχου των δεδομένων για τη διατήρηση της εμπιστευτικότητας αυτών […], δεν έχει σημασία εάν η προστασία των δεδομένων από τη μη εξουσιοδοτημένη πρόσβαση παρακάμπτεται αργά ή γρήγορα, με πολύ ή με λίγο κόπο. Πρόθεση του νομοθέτη, σύμφωνα με το Δικαστήριο, ήταν να αποκλείσει από το πεδίο της αντικειμενικής υπόστασης, πέρα από τις περιπτώσεις ήσσονος σημασίας, μόνον εκείνες στις οποίες η υπέρβαση του μέτρου προστασίας είναι δυνατή για τον καθένα χωρίς περαιτέρω ενέργειες. Δεν επιθυμούσε, όμως, να αποκλείσει τις περιπτώσεις στις οποίες τα μέτρα προστασίας παρακάμπτονται με ευκολία

λόγω ιδιαίτερων γνώσεων ή δυνατοτήτων συγκεκριμένων δραστών. Μόνον αυτή η γενική-αφηρημένη θεώρηση είναι συμβατή με τον σκοπό του νόμου.

2) Τούτων δοθέντων, ο κατηγορούμενος Η υπερέβη το μέτρο προστασίας. Παρέκαμψε τον κωδικό προστασίας των προσωπικών λογαριασμών ηλεκτρονικού ταχυδρομείου, διότι ως διαχειριστής απέκτησε πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου των συνεργατών του τροποποιώντας παράνομα τη ρύθμιση «Δικαιούχοι Πρόσβασης». Ο δικαιούχος των δεδομένων ήθελε προφανώς να εμποδίσει αυτή τη μορφή πρόσβασης μέσω του ξεκάθαρου περιορισμού των δικαιωμάτων των διαχειριστών και την πρόβλεψη συγκεκριμένης διαδικασίας για την προσπέλαση των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το γεγονός ότι η υπέρβαση του μέτρου προστασίας έλαβε χώρα με μερικά κλικ του ποντικιού δεν αποκλείει τη στοιχειοθέτηση του αδικήματος του άρθρου 202a παρ. 1 γερμΠΚ.

δδ) Τα ανωτέρω έπραξε ο δράστης χωρίς δικαίωμα […], διότι η κατ' αυτόν τον τρόπο απόκτηση πρόσβασης στο περιεχόμενο των μηνυμάτων ηλεκτρονικού ταχυδρομείου απαγορευόταν.

γ) Ωστόσο, η απόφαση για τη δήμευση μπορεί να διατηρηθεί μόνο για ποσό ύψους 53.300 ευρώ. Ορθά υποστηρίζει ο κατηγορούμενος Η με την αίτηση αναίρεσης ότι εν προκειμένω δεν είναι δυνατόν να επιβληθεί δήμευση για τις πράξεις για τις οποίες έχει αποφασιστεί αποχή από την ποινική δίωξη κατά το άρθρο 154 παρ. 2 γερμΚΠΔ. Το Τμήμα έχει αφαιρέσει το ποσό που αναφέρεται σε αυτές τις πράξεις από το κατά τα λοιπά ορθώς υπολογισθέν συνολικό ποσό (52.300 ευρώ για την πράξη της κλοπής με διάρρηξη και 1.000 ευρώ για τις πράξεις των περιπτώσεων 28 και 40).

δ) Δεν είναι άδικο να επιβαρυνθεί ο Η με τα δικαστικά έξοδα, εφόσον το ένδικο μέσο που άσκησε είχε μόνον εν μέρει αποτέλεσμα.

Β) Αίτηση αναίρεσης του κατηγορουμένου Β

1. Η απόφαση του Πρωτοδικείου περί συναυτουργίας του κατηγορουμένου Β στις ως άνω πράξεις είναι αναιρετέα […].

Ο κατηγορούμενος Β δεν άσκησε και ούτε θα μπορούσε να είχε ασκήσει οποιαδήποτε επιρροή στον συγκεκριμένο τρόπο τέλεσης του εγκλήματος της υποκλοπής δεδομένων. Ο Β δεν γνώριζε με ποιον τρόπο ο Η θα υπερέβαινε ένα πιθανό μέτρο προστασίας. Απλώς υπέθετε ότι ο τελευταίος πιθανόν να χρειαζόταν «να κάνει κάποιο κόλπο». Ο Β είχε, όμως, ιδιαίτερο συμφέρον από το αποτέλεσμα της πράξης και άσκησε επιρροή ώστε να ενεργήσει ο Η μέσω της υπόσχεσης αμοιβής και μέσω της υπόδειξης λογαριασμών ηλεκτρονικού ταχυδρομείου

που θα αποτελούσαν αντικείμενο υποκλοπής. Έτσι, όμως, [εννοείται: η δράση του Β] δεν διαφοροποιείται από άλλες περιπτώσεις ηθικών αυτουργών που ενδιαφέρονται για το αποτέλεσμα, αλλά δεν επηρεάζουν τον δράστη ως προς τον συγκεκριμένο τρόπο τέλεσης […].

2. Οι διαπιστώσεις [εννοείται: του Πρωτοδικείου] δεν θίγονται από αυτό το σφάλμα αξιολόγησης (βλ. το άρθρο 353 παρ. 2 γερμΚΠΔ). Η αναίρεση του κατηγορουμένου είναι αβάσιμη.

3. Το Τμήμα εξέτασε κατά πόσον θα μετατρέψει κατ' άρθρο 354 παρ. 1 γερμΚΠΔ την καταδικαστική κρίση [εννοείται: εις βάρος του Β] σε ηθική αυτουργία σε υποκλοπή δεδομένων επί τη βάσει των ορθών διαπιστώσεων [εννοείται: του Πρωτοδικείου]. Η μετατροπή αυτή δεν κωλύεται από το γεγονός ότι ο Η ήταν πιθανότατα έτοιμος για την τέλεση των αδικημάτων, είχε επιδείξει αυτήν την ετοιμότητα και είχε ο ίδιος την πρωτοβουλία για την τέλεση των πράξεων […]. Αρκεί ότι ο Β, όπως διαπιστώθηκε, προκάλεσε εν προκειμένω [εννοείται: στον Η] την απόφαση για την τέλεση της πράξης με την υπόδειξη των λογαριασμών ηλεκτρονικού ταχυδρομείου που θα αποτελούσαν αντικείμενο υποκλοπής. Εντούτοις, το Τμήμα δεν επιτρέπεται να προβεί σε αυτή τη μετατροπή της καταδικαστικής κρίσης [εννοείται: εις βάρος του Β] λόγω της εφαρμογής του άρθρου 265 παρ. 1 γερμΚΠΔ, διότι δεν μπορεί να αποκλειστεί ότι ο Β θα μπορούσε να είχε ασκήσει διαφορετικά, ίσως δε πιο αποτελεσματικά, τα υπερασπιστικά του δικαιώματα έναντι αυτής της κατηγορίας.

Παρατηρήσεις

1. Η κρίση του γερμανικού Ακυρωτικού

Σύμφωνα με το ιστορικό τής υπό στοιχεία 5 StR 614/19 απόφασης του γερμανικού Ακυρωτικού, οι δράστες συνήψαν την ακόλουθη συμφωνία: Ο Η, τεχνικός υπολογιστών και διαχειριστής του πληροφοριακού συστήματος του Ομοσπονδιακού Υπουργείου Υγείας, θα εκμεταλλευόταν τη θέση του προκειμένου να αντιγράψει σε οπτικό δίσκο μηνύματα ηλεκτρονικού ταχυδρομείου συνεργατών του στο Υπουργείο, αλλά και του ίδιου του Υπουργού, και να τα παραδώσει έναντι αμοιβής στον Β. Ο τελευταίος θα «ενημέρωνε» τον ιστότοπό του με τις απόρρητες πληροφορίες με σκοπό να αποκτήσει οικονομικό όφελος από την αυξημένη επισκεψιμότητα.

Η ως άνω απόφαση του γερμανικού Ακυρωτικού παρουσιάζει ενδιαφέρον για τους ακόλουθους λόγους: Πρώτον, διότι το Δικαστήριο απεφάνθη για την έννοια των μέτρων προστασίας που έπρεπε να έχει λάβει ο νόμιμος κάτοχος των δεδομένων, ώστε να στοιχειοθετείται το αδίκημα της υποκλοπής δεδομένων (άρθρο 202a γερμΠΚ, Υποκλοπή Δεδομένων - Ausspähen von

Daten).[4] Σημειωτέον ότι και στον ελληνικό Ποινικό Κώδικα προβλέπεται ως προϋπόθεση για τη στοιχειοθέτηση των αδικημάτων των άρθρων 370Β παρ. 1 και 370Δ παρ. 2 ΠΚ η λήψη μέτρων προστασίας ή ασφαλείας από το θύμα. Δεύτερον, γιατί στην απόφαση θίγεται το ζήτημα της τέλεσης του αδικήματος του άρθρου 202a γερμΠΚ αλλά και των αδικημάτων των άρθρων 370Β, 370Γ και 370Δ ΠΚ από δράστη που βρίσκεται στην υπηρεσία του κατόχου των δεδομένων.[5] Τρίτον, διότι τα γενόμενα δεκτά πραγματικά περιστατικά δίνουν αφορμή για προβληματισμό για το αξιόποινο της αποδοχής δεδομένων που έχουν αποκτηθεί από παράνομη πράξη στην ελληνική έννομη τάξη.

Όσον αφορά το πρώτο ζήτημα, το γερμανικό Ακυρωτικό έκρινε ότι το Ομοσπονδιακό Υπουργείο Υγείας είχε πράγματι λάβει μέτρα προστασίας έναντι της μη εξουσιοδοτημένης πρόσβασης επί των δεδομένων των πληροφοριακών του συστημάτων, με βάση δύο κριτήρια.

Σύμφωνα με το πρώτο, αντικειμενικό κριτήριο, αρκεί για την ύπαρξη μέτρου προστασίας να έχει τεθεί κάποιο εμπόδιο που αποτρέπει ή τουλάχιστον δυσχεραίνει την προσπέλαση των δεδομένων από τον δράστη. Δεν ασκεί επιρροή εάν ο συγκεκριμένος δράστης μπορεί να υπερβεί το εμπόδιο εύκολα ή δύσκολα. Αρκεί το εμπόδιο αυτό να υφίσταται αντικειμενικά. Αντιθέτως, δεν πληρούται η αντικειμενική υπόσταση του εγκλήματος του άρθρου 202a γερμΠΚ, όταν ο δράστης έχει ακώλυτη πρόσβαση επί των δεδομένων.

Σύμφωνα με το δεύτερο, υποκειμενικό κριτήριο, ο δράστης πρέπει διά της υπερβάσεως του εμποδίου να εξαναγκάζεται «σε μια μορφή πρόσβασης επί των δεδομένων, την οποία ο νόμιμος κάτοχος θέλει καταφανώς να εμποδίσει». Απαιτείται, αλλά ταυτόχρονα αρκεί, ο νόμιμος κάτοχος των δεδομένων να εκφράζει με το μέτρο προστασίας τη βούλησή του για την προστασία του απορρήτου.

Εφαρμόζοντας, λοιπόν, τα ανωτέρω κριτήρια, το γερμανικό Ακυρωτικό έκρινε ότι η εφαρμογή κωδικού συνιστά «μέτρο προστασίας» έναντι της μη εξουσιοδοτημένης πρόσβασης επί των δεδομένων, ακόμη κι αν ο συγκεκριμένος δράστης δύναται, ενόψει των ιδιαίτερων γνώσεων ή δυνατοτήτων του, να το παρακάμψει γρήγορα και εύκολα.[6]
Περαιτέρω, το Δικαστήριο έκρινε ότι στοιχειοθετείται το αδίκημα του άρθρου 202a γερμΠΚ (Υποκλοπή Δεδομένων - Ausspähen von Daten) παρότι ο δράστης βρισκόταν στην υπηρεσία

4. Άρθρο 202a παρ. 1 γερμΠΚ: «Όποιος αποκτά για τον εαυτό του ή για άλλον χωρίς δικαίωμα και διά της υπερβάσεως μέτρων προστασίας πρόσβαση σε δεδομένα, τα οποία δεν προορίζονται γι' αυτόν και είναι ιδιαιτέρως προστατευμένα έναντι της μη εξουσιοδοτημένης πρόσβασης τιμωρείται με στερητικής της ελευθερίας ποινή έως τριών ετών ή με χρηματική ποινή. […]».

5. *Bosch,* Ausspähen von Daten durch Systemadministrator, JURA 2020, 1145.

6. Βλ. επίσης *Hilgendorf/Valerius,* Computer- und Internetstrafrecht, ²2012, σ. 165.

του νόμιμου κατόχου των δεδομένων. Σημειωτέον ότι στο παρελθόν είχε κριθεί ότι δεν πληρούται η αντικειμενική υπόσταση του εγκλήματος, όταν ο ευρισκόμενος στην υπηρεσία του κατόχου των δεδομένων δράστης χρησιμοποιεί τα αποθηκευμένα στα πληροφοριακά συστήματα του κατόχου δεδομένα για ιδιωτικούς σκοπούς.[7] Η θέση αυτή υποστηρίζεται και στη γερμανική θεωρία με το επιχείρημα ότι όταν ο δράστης έχει ήδη ακώλυτη πρόσβαση στα αποθηκευμένα δεδομένα, η πράξη του μπορεί να συνιστά απιστία έναντι του εργοδότη ή παραβίαση των κανόνων περί αθεμίτου ανταγωνισμού, αλλά όχι υποκλοπή δεδομένων.[8]

Το γερμανικό Ακυρωτικό έλαβε υπόψη ότι το Ομοσπονδιακό Υπουργείο Υγείας είχε προηγουμένως περιορίσει τα δικαιώματα πρόσβασης των διαχειριστών του συστήματος. Ο νόμιμος κάτοχος είχε, επομένως, προσδιορίσει σε ποια στοιχεία επιτρέπεται να έχουν πρόσβαση οι διαχειριστές και σε ποιες μορφές επεξεργασίας μπορούν να προβούν. Συγκεκριμένα, είχε απαγορεύσει στους διαχειριστές την πρόσβαση αλλά και την ανάγνωση και αντιγραφή των μηνυμάτων από τους ιδιωτικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου των συνεργατών του Υπουργείου.[9]

Υπ' αυτήν την έννοια, τα συγκεκριμένα στοιχεία δεν «προορίζονταν» κατά την έννοια του άρθρου 202a γερμΠΚ για επεξεργασία από τους διαχειριστές, και τυχόν παραβίαση των τεθειμένων κωδικών πρόσβασης συνιστούσε υπέρβαση μέτρου προστασίας, ακόμη κι αν οι κωδικοί παρακάμφθηκαν με ευκολία.

2. Αξιολόγηση των πραγματικών περιστατικών

Τόσο τα πραγματικά περιστατικά που τέθηκαν υπόψη του γερμανικού Ακυρωτικού όσο και η κρίση του Δικαστηρίου παρουσιάζουν ενδιαφέρον για την ελληνική έννομη τάξη.

Επισημαίνεται εξαρχής ότι στην ελληνική έννομη τάξη η συμπεριφορά των Η και Β θα έπρεπε να αξιολογηθεί με βάση τα άρθρα 370Β, 370Γ και 370Δ ΠΚ. Τα τρία αυτά άρθρα αποτελούν τις βασικές ποινικές διατάξεις που τιμωρούν τη χωρίς δικαίωμα απόκτηση πρόσβασης σε ηλεκτρονικά δεδομένα, πληροφοριακά συστήματα, στοιχεία που μεταδίδονται μέσω συστημάτων τηλεπικοινωνιών και απόρρητα στην ελληνική έννομη τάξη.[10]

7. Βλ. ιδίως BayObIG NJW 1999, 1727-1728. Η απόφαση παρουσιάζεται και από τον *Φιλόπουλο* (Ποινική Προστασία Απορρήτου, 2015, σ. 178).

8. Βλ. *Hilgendorf,* σε: Leipziger Kommentar, [12]2009, άρθρο 202a πλαγιάρ. 23-24, *Heiming,* Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, 1995, σ. 54-55.

9. Σχετική η ΤρΝαυτΠειρ 530/2003 ΠοινΧρ 2004, 75, με την οποία κελευστής καταδικάστηκε για παράνομη χρησιμοποίηση προγράμματος υπολογιστή, διότι έθεσε σε λειτουργία τον ηλεκτρονικό υπολογιστή και χρησιμοποιώντας εγκατεστημένο πρόγραμμα προέβη σε εκτύπωση ορισμένων εγγράφων, ενώ ο ίδιος δεν περιλαμβανόταν στο εξουσιοδοτημένο προσωπικό.

10. Ορθά σημειώνεται από την *Καμπέρου* [σε: Χαραλαμπάκη (εκδ. επιμ.), ΕρμΠΚ 2021, άρθρο 370Δ πλαγιάρ. 11] ότι οι

Τα γενόμενα δεκτά από το γερμανικό Ακυρωτικό πραγματικά περιστατικά θα μπορούσαν να υπαχθούν στην ειδική υπόσταση των αδικημάτων των άρθρων 370 παρ. 2, 370Β παρ. 1, 2, 4 και 370Δ παρ. 2, 3 ΠΚ, καθώς ο Η, ευρισκόμενος στην υπηρεσία του νόμιμου κατόχου των δεδομένων, απέκτησε χωρίς δικαίωμα πρόσβαση τουλάχιστον σε μέρος πληροφοριακού συστήματος και σε ηλεκτρονικά δεδομένα, καθ' υπέρβαση μέτρων προστασίας και μέτρων ασφαλείας.

Αντιθέτως, δεν θα ετίθετο ζήτημα εφαρμογής του άρθρου 370Γ παρ. 2 ΠΚ,[11] αφού στα μηνύματα ηλεκτρονικού ταχυδρομείου δεν περιλαμβάνονταν κρατικά[12] ή επιστημονικά απόρρητα. Επιπλέον, τα δεδομένα που παρανόμως απέκτησε ο Η δεν μπορούν να χαρακτηριστούν ως επαγγελματικά απόρρητα. Ως επαγγελματικά απόρρητα ορίζονται κατ' ορθότερη άποψη τα στοιχεία που καταγράφει και αποθηκεύει ο επαγγελματίας-λειτουργός λόγω του επαγγέλματός του.[13] Αποτελούν, λοιπόν, επαγγελματικό απόρρητο οι σημειώσεις του ιατρού κατά την εξέταση του ασθενούς, αλλά όχι οι διαπραγματεύσεις του Υπουργείου με εκπροσώπους επαγγελματικών κλάδων. Εξάλλου, το Υπουργείο Υγείας δεν μπορεί να χαρακτηριστεί ως επιχείρηση του δημοσίου τομέα.

Όσον αφορά τη σχέση των ως άνω διατάξεων του Ποινικού Κώδικα παρατηρείται ότι αυτές προστατεύουν το ίδιο έννομο αγαθό, δηλαδή το τυπικό δικαίωμα του νόμιμου κατόχου των πληροφοριακών συστημάτων, των ηλεκτρονικών δεδομένων και των απορρήτων να αποκλείει άλλους από την πρόσβαση σε αυτά.[14] Επιπλέον, οι αντικειμενικές υποστάσεις των εγκλημάτων αυτών δεν συνδέονται με σχέση ειδικότητας, αφού καμία εξ αυτών δεν περιλαμβάνει εν μέρει όλα τα στοιχεία άλλης. Συνεπώς, στην προκειμένη περίπτωση εφαρμοστέα θα ήταν η διάταξη του άρθρου 370Β παρ. 4 ΠΚ, διότι σε αυτήν προβλέπεται βαρύτερη ποινή.[15]

διατάξεις των άρθρων 370Β παρ. 1 ΠΚ και 370Δ παρ. 2 ΠΚ επικαλύπτονται όσον αφορά τη χωρίς δικαίωμα απόκτηση πρόσβασης σε σύνολο ή τμήμα πληροφοριακού συστήματος.

11. Κατά την *Καϊάφα-Γκμπάντι,* η αντικειμενική υπόσταση του άρθρου αυτού «περιορίζεται με μια λογικοσυστηματική ερμηνεία σε περιπτώσεις παράνομης διείσδυσης σε κρατικά, επιστημονικά, επαγγελματικά ή επιχειρησιακά απόρρητα, καλύπτοντας έτσι περιπτώσεις της διαδεδομένης εμπορικής, βιομηχανικής κ.λπ. κατασκοπείας». Βλ. *Καϊάφα-Γκμπάντι,* Η ποινική αντιμετώπιση των επιθέσεων κατά των συστημάτων πληροφοριών στο πλαίσιο της Ε.Ε. και η αναμενόμενη επίδρασή της στην ελληνική έννομη τάξη, ΠοινΧρ 2011, 489 επ., 497. Σημειωτέον ότι το σημερινό άρθρο 370Γ αντιστοιχούσε στο άρθρο 370Β ΠΚ 1950.

12. Η έννοια του «κρατικού απορρήτου» ορίζεται στο άρθρο 149 ΠΚ: «Κρατικό απόρρητο κατά την έννοια των άρθρων 146 έως 148 είναι ένα γεγονός, αντικείμενο ή πληροφορία, η πρόσβαση στα οποία είναι δυνατή σε ένα προσδιορισμένο κύκλο προσώπων και που χαρακτηρίζονται ως μυστικά για να αποφευχθεί ο κίνδυνος προσβολής της εδαφικής ακεραιότητας, της αμυντικής ικανότητας, των διεθνών σχέσεων ή των οικονομικών συμφερόντων του ελληνικού κράτους και της διεθνούς ειρήνης».

13. *Φιλόπουλος,* ό. π., σ. 151-152.

14. *Μυλωνόπουλος,* Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο, σειρά ΠΟΙΝΙΚΑ αριθμ. 33, 1991, σ. 92.

15. Βλ. *Καμπέρου* [σε: Χαραλαμπάκη (εκδ. επιμ.), ΕρμΠΚ 2021, άρθρο 370Β πλαγιάρ. 21, άρθρο 370Δ πλαγιάρ. 11]

3. Η έννοια των «μέτρων προστασίας»

Η απόφαση του γερμανικού Ακυρωτικού μπορεί να αξιοποιηθεί για την ερμηνεία του όρου «μέτρα προστασίας» του άρθρου 370Β παρ. 1 ΠΚ. Ταυτόσημος πρέπει να θεωρείται ο όρος «μέτρα ασφαλείας» του άρθρου 370Δ παρ. 2 ΠΚ. Η χρήση, όμως, διαφορετικής ορολογίας προβληματίζει. Ορθά επισημαίνεται ότι όταν ο νομοθέτης απαιτεί από τον παθόντα να έχει λάβει μέτρα για την προστασία του εννόμου αγαθού, όπως λ.χ. τα προβλεπόμενα στις ως άνω διατάξεις, εφαρμόζει τη θυματοδογματική αρχή.[16]

Εντούτοις, δεν μπορεί να απαιτηθεί από τον παθόντα να λαμβάνει εξειδικευμένα μέτρα προστασίας. Το κρίσιμο στοιχείο είναι να καθίσταται σαφής η βούληση του νόμιμου κατόχου να προστατεύσει το απόρρητο των δεδομένων και όχι οι δυνατότητες του συγκεκριμένου δράστη in concreto. Αρκούν απλά μέτρα, ακόμη κι αν αυτά μπορούν να παρακαμφθούν με ευκολία από δράστες με ιδιαίτερες τεχνικές γνώσεις.[17]

Τα μέτρα προστασίας του πληροφοριακού συστήματος ή των ηλεκτρονικών δεδομένων μπορούν να κατηγοριοποιηθούν σε α) μέτρα που τίθενται επί του υλισμικού (Hardware), όπως λ.χ. συστήματα αναγνώρισης δακτυλικού αποτυπώματος, ίριδας ή άλλων βιομετρικών στοιχείων, β) μέτρα που τίθενται επί του λογισμικού (Software), όπως λ.χ. κωδικοί πρόσβασης, γ) οικοδομικά μέτρα ασφαλείας που αποσκοπούν στην προστασία του υλικού φορέα του πληροφοριακού συστήματος, όπως λ.χ. η τοποθέτηση κλειδαριάς ασφαλείας στον χώρο που βρίσκεται το πληροφοριακό σύστημα, δ) μέτρα κρυπτογράφησης των ηλεκτρονικών δεδομένων.[18]
Δεν αποτελούν, ωστόσο, "μέτρα ασφαλείας" ή "μέτρα προστασίας" τα μέτρα που εμφανώς προορίζονται για την αποτροπή άλλων κινδύνων, όπως λ.χ. πυρκαγιά ή πλημμύρα.[19]

εφαρμόζοντας την αρχή της σιωπηρής επικουρικότητας.

16. Επ' αυτού βλ. *Hilgendorf,* σε: Leipziger Kommentar, [12]2009, άρθρο 202a πλαγιάρ. 29, *Schünemann,* Der strafrechtliche Schutz von Privatgeheimnissen, ZStW 1978, 11 επ., ιδίως 32. Βλ. επίσης *Φιλόπουλου,* ό. π., σ. 183.

17. *Kindhäuser/Schramm,* Strafrecht BT I, [9]2020, σ. 240, *Heiming,* ό. π., σ. 71.

18. Για την κατηγοριοποίηση αυτή, βλ. *Hilgendorf,* σε: Leipziger Kommentar, [12]2009, άρθρο 202a πλαγιάρ. 34. Για τα μέτρα προστασίας, βλ. *Μυλωνόπουλου,* ό. π., σ. 97-98 και *Φιλόπουλου,* ό. π., σ. 155-156 και 183-184, *Σπυρόπουλου,* Χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά συστήματα πληροφοριών (Hacking), σειρά ΠΟΙΝΙΚΑ αριθμ. 86, 2016, σ. 197. Για το Firewall ως μέτρο προστασίας, βλ. και *Κουτσουπιά,* Ζητήματα δήμευσης κρυπτονομισμάτων ως προϊόντων του εγκλήματος, ΠοινΧρ 2021, 717 επ.

19. *Φιλόπουλος,* ό. π., σ. 155.

4. Ο δράστης που βρίσκεται στην υπηρεσία του νόμιμου κατόχου

Με την υπό στοιχεία 5 StR 614/19 απόφαση, το γερμανικό Ακυρωτικό απεφάνθη ότι είναι νοητή η χωρίς δικαίωμα απόκτηση πρόσβασης σε δεδομένα από δράστη που βρίσκεται στην υπηρεσία του νόμιμου κατόχου, εφόσον αυτός υπερβαίνει κάποιο μέτρο προστασίας.

Ο Έλληνας νομοθέτης έχει θεσπίσει ειδικές προβλέψεις στα άρθρα 370Β, 370Γ και 370Δ ΠΚ για τις περιπτώσεις κατά τις οποίες ο δράστης βρίσκεται στην υπηρεσία του κατόχου των δεδομένων.

Στο άρθρο 370Β παρ. 2 ΠΚ, προβλέπεται ότι «αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του συστήματος πληροφοριών ή των δεδομένων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του». Παρόμοια πρόβλεψη υπάρχει και στο άρθρο 370Δ παρ. 3 ΠΚ.

Επιπλέον, με το άρθρο 370Β παρ. 4 ΠΚ εισάγεται διακεκριμένη παραλλαγή, σύμφωνα με την οποία «αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής αξίας, επιβάλλεται φυλάκιση και χρηματική ποινή». Παρόμοια ρύθμιση εντοπίζεται και στο άρθρο 370Γ παρ. 2 ΠΚ, όχι όμως στο άρθρο 370Δ ΠΚ.

Ο νομοθέτης έχει θέσει, επομένως, μία επιπλέον προϋπόθεση για τη στοιχειοθέτηση του αδικήματος του άρθρου 370Β ΠΚ, όταν ο δράστης βρίσκεται στην υπηρεσία του νόμιμου κατόχου. Απαιτείται, δηλαδή, η πράξη του δράστη να παραβιάζει τον εσωτερικό κανονισμό ή την έγγραφη εντολή του νόμιμου κατόχου ή αρμόδιου υπαλλήλου.

Συνεπώς, για τη στοιχειοθέτηση του αδικήματος του άρθρου 370Β παρ. 4 ΠΚ, απαιτούνται σωρευτικά: α) ο δράστης να βρίσκεται στην υπηρεσία του νόμιμου κατόχου. Κατά μία άποψη, αρκεί ο δράστης να «συνδέεται με τον κάτοχο με οποιαδήποτε σχέση εξαρτημένης ή ανεξάρτητης εργασίας, ή ακόμη και με σύμβαση έργου, ανεξαρτήτως αν η εργασία ανήκει στον δημόσιο ή στον ιδιωτικό τομέα».[20] Υποστηρίζεται, ωστόσο, η θέση ότι μεταξύ του νόμιμου κατόχου

20. *Κωστάρας,* ΕιδΠοιν, [4]2014, σ. 1149. Βλ. επίσης *Βασιλάκη,* Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, σειρά ΠΟΙΝΙΚΑ αριθμ. 40, 1993, σ. 183. *Καμπέρου,* σε: Χαραλαμπάκη (εκδ. επιμ.), ΕρμΠΚ 2021, άρθρο 370Β πλαγιάρ. 17.

και του δράστη πρέπει να υφίσταται σχέση εξαρτημένης εργασίας.[21] Δεν μπορούν πάντως κατ' ορθότερη άποψη να αποτελέσουν υποκείμενα του εγκλήματος τα μέλη του ΔΣ της επιχείρησης, διότι δεν βρίσκονται στην υπηρεσία του νόμιμου κατόχου.[22] Επιπλέον, απαιτείται β) ο δράστης να αποκτά πρόσβαση σε μέρος ή στο σύνολο πληροφοριακού συστήματος ή σε ηλεκτρονικά δεδομένα, γ) υπερβαίνοντας μέτρο προστασίας που έχει τεθεί από τον νόμιμο κάτοχο και δ) παραβιάζοντας τον εσωτερικό κανονισμό ή την έγγραφη εντολή του νόμιμου κατόχου ή αρμόδιου υπαλλήλου.

Τίθεται, όμως, το ερώτημα αν ο εσωτερικός κανονισμός αποτελεί μέτρο ασφαλείας. Η απάντηση στο ερώτημα αυτό πρέπει να είναι αρνητική. Τα μέτρα προστασίας προστατεύουν τα ηλεκτρονικά δεδομένα και τα πληροφοριακά συστήματα από τη μη εξουσιοδοτημένη πρόσβαση, ενώ ο εσωτερικός κανονισμός καταδεικνύει *πότε* η πρόσβαση του δράστη που βρίσκεται στην υπηρεσία του νόμιμου κατόχου είναι μη εξουσιοδοτημένη. Ο νομοθέτης απαιτεί η πράξη του δράστη που βρίσκεται στην υπηρεσία του νόμιμου κατόχου να παραβιάζει τον εσωτερικό κανονισμό, διότι αναγνωρίζει ότι συνήθως οι εργαζόμενοι αποκτούν de facto πρόσβαση στα πληροφοριακά συστήματα και τα ηλεκτρονικά δεδομένα του εργοδότη-νόμιμου κατόχου.[23] Ο εσωτερικός κανονισμός (ή αντίστοιχα η έγγραφη εντολή του νόμιμου κατόχου ή του αρμόδιου υπαλλήλου) καταδεικνύει, λοιπόν, σε αυτές τις περιπτώσεις πότε ο δράστης πράττει χωρίς δικαίωμα.

Σε αντίθεση, όμως, προς το άρθρο 370Β, το αδίκημα του άρθρου 370Δ παρ. 2, 3 ΠΚ στοιχειοθετείται και μόνο διά της παραβιάσεως του εσωτερικού κανονισμού από τον δράστη που βρίσκεται στην υπηρεσία του νόμιμου κατόχου. Στο συμπέρασμα αυτό οδηγείται κανείς εάν λάβει υπόψη ότι ο νομοθέτης αρκείται στην παραβίαση απαγορεύσεων για τη στοιχειοθέτηση του αδικήματος. Ως «απαγορεύσεις» ορίζονται «οι ρητές εντολές, γραπτές ή προφορικές, σχετικά με την αποτροπή μη δικαιούχων από την πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών».[24] Συνεπώς, ο εσωτερικός κανονισμός και οι έγγραφες εντολές του νόμιμου κατόχου με τις οποίες καθορίζονται κανόνες για την πρόσβαση στο σύστημα πληροφοριών αποτελούν «απαγορεύ-

21. *Μυλωνόπουλος,* ό. π., σ. 84, *Φιλόπουλος,* ό. π., σ . 190-191, με το επιχείρημα ότι τότε μόνον η απαγόρευση πρόσβασης είναι δεσμευτική.

22. *Μυλωνόπουλος,* ό. π., σ. 84.

23. *Βασιλάκη,* ό. π., σ. 92. Η συγγραφέας παρατηρεί ότι η προϋπόθεση παραβίασης του εσωτερικού κανονισμού ή έγγραφης εντολής αποτελεί «ειδικό λόγο περιορισμού της αντικειμενικής υπόστασης» που αποσκοπεί στην αποφυγή μιας υπερποινικοποίησης.

24. *Φιλόπουλος,* ό. π., σ. 183.

σεις» εν τη εννοία του άρθρου 370Δ παρ. 3 ΠΚ. Παραμένει, ωστόσο, άδηλο για ποιον λόγο η παραβίαση απαγορεύσεων αρκεί για τη στοιχειοθέτηση του αδικήματος του άρθρου 370Δ παρ. 2, 3 ΠΚ αλλά όχι για τη στοιχειοθέτηση του αδικήματος του άρθρου 370Β παρ. 1, 2, 4 ΠΚ.

Τέλος, αξίζει να σημειωθεί ότι μέχρι σήμερα δεν εντοπίζονται πολλές νομολογιακές περιπτώσεις απόκτησης πρόσβασης χωρίς δικαίωμα σε μέρος ή σύνολο πληροφοριακού συστήματος, ή σε ηλεκτρονικά δεδομένα, ή σε απόρρητα από δράστη που βρίσκεται στην υπηρεσία του νόμιμου κατόχου.[25] Έχει, όμως, κριθεί ότι στοιχειοθετείται το αδίκημα του άρθρου 370Β ΠΚ 1950,[26] όταν υπάλληλοι με σύμβαση εξαρτημένης εργασίας αντιγράφουν σε δισκέτες το πελατολόγιο της εταιρίας με σκοπό να το χρησιμοποιήσουν σε ανταγωνιστική επιχείρηση που ίδρυσαν[27] ή όταν προγραμματιστής ασφαλιστικών εταιρειών αντιγράφει χωρίς δικαίωμα από τους ηλεκτρονικούς υπολογιστές των εταιρειών απόρρητα στοιχεία πελατών και τα αποκαλύπτει σε τρίτους έναντι αμοιβής.[28] Σχετική είναι επίσης και παλαιότερη απόφαση, κατά την οποία τέλεσε το αδίκημα του άρθρου 370 ΠΚ λογιστής επιχείρησης που έλαβε αντίγραφα εγγράφων, γνωρίζοντας ότι αυτά δεν προορίζονταν για να περιέλθουν σε γνώση του, και τα χρησιμοποίησε ως αποδεικτικό μέσο για την υποστήριξη της αγωγής του κατά του εργοδότη του.[29]

5. Παράνομη αποδοχή παρανόμως κτηθέντων ηλεκτρονικών δεδομένων, στοιχείων υπολογιστή ή απορρήτων

Τέλος, η ως άνω απόφαση του γερμανικού Ακυρωτικού θέτει ένα ακόμα ενδιαφέρον ζήτημα: Ποια είναι η ευθύνη του δράστη που αποκτά έναντι τιμήματος ή εν γένει αποδέχεται δεδομένα που έχουν αποκτηθεί χωρίς δικαίωμα;

Στην ελληνική έννομη τάξη, δεν υπάρχει διάταξη αντίστοιχη του άρθρου 202d (Αποδοχή παρανόμως κτηθέντων δεδομένων – Datenhehlerei), σύμφωνα με το οποίο τιμωρείται όποιος αποκτά

25. Από τη νομολογία των πολιτικών δικαστηρίων, βλ. ΜΠρΠειρ 4138/2019 ΤΝΠ ΝΟΜΟΣ, στην οποία αναφέρεται ότι «η εργαζόμενη παράνομα και υπαίτια ενήργησε, στοιχειοθετούμενου του αδικήματος του άρθρου 370Β ΠΚ, αφού αθέμιτα αντέγραψε στοιχεία υπολογιστών, τα οποία συνιστούν επαγγελματικά απόρρητα, εφόσον παρανόμως μεταφέρθηκαν εκτός ηλεκτρονικών συστημάτων εταιρίας, με προφανή σκοπό να χρησιμοποιηθούν από την ανταγωνίστρια εταιρίας στην οποία θα προσλαμβανόταν». Παρομοίως, ΕφΠατρ 9/2001 ΤΝΠ ΝΟΜΟΣ.

26. Υπενθυμίζεται ότι το άρθρο 370Γ ΠΚ αντιστοιχεί στο άρθρο 370Β ΠΚ 1950. Επ' αυτού, βλ. το άρθρο 370Γ της αιτιολογικής έκθεσης του Ποινικού Κώδικα 2019.

27. ΑΠ 121/2003 ΠοινΧρ 2003, 910, με παρατ. Κωνσταντινίδη.

28. ΣυμβΕφΑθ 217/1997 με εισ. πρότ. Β. Μαρκή, ΠοινΧρ 1997, 876. Βλ. ιδίως *Κωνσταντινίδη,* Η διακεκριμένη παραβίαση απόρρητων στοιχείων (άρθρο 370Β § 2 περ. β' ΠΚ), ΠοινΧρ 1997, 1216 επ.

29. ΣυμβΠλημΠειρ 345/1962 με εισ. πρότ. Α. Πολυχρονόπουλου, ΠοινΧρ 1962, 240-241.

για τον εαυτό του ή για άλλον, ή μεταδίδει σε άλλον, ή διαδίδει, ή κατ' άλλον τρόπο καθιστά προσιτά δεδομένα που δεν είναι γενικώς προσπελάσιμα και τα οποία άλλος έχει αποκτήσει με παράνομη πράξη, για να αποκτήσει ο ίδιος ή άλλος περιουσιακό όφελος ή για να βλάψει άλλον. Επιπροσθέτως, πρέπει να γίνει δεκτό ότι τα δεδομένα, ακόμη κι αν αποθηκεύονται σε υλικό φορέα αποθήκευσης (όπως λ.χ. οπτικός δίσκος), δεν καθίστανται πράγματα εν τη εννοία του άρθρου 394 ΠΚ και του άρθρου 947 ΑΚ.[30] Ο αποδεχόμενος υλικό φορέα αποθήκευσης θα μπορούσε, εφόσον πληρούνται και οι λοιποί όροι της ειδικής υπόστασης του εγκλήματος, να τιμωρηθεί μόνο για την αποδοχή του οπτικού δίσκου ή του εξωτερικού σκληρού δίσκου και όχι για την αποδοχή των αποθηκευμένων δεδομένων.[31]

Εντούτοις, τα δεδομένα έχουν συχνά μεγαλύτερη οικονομική αξία σε σχέση με τους φορείς στους οποίους είναι αποθηκευμένα. Παρουσιάζεται, λοιπόν, αξιολογική αντινομία, αφού ο Έλληνας νομοθέτης τιμωρεί το έλασσον, δηλαδή την αποδοχή του φορέα αποθήκευσης, αλλά όχι το μείζον, ήτοι την αποδοχή των αποθηκευμένων δεδομένων.

Το τιμωρητικό αυτό έλλειμμα καλύπτεται, όταν στα δεδομένα που αποδέχεται ο δράστης περιλαμβάνονται: α) προσωπικά δεδομένα, αφού τότε εφαρμόζεται η διάταξη του άρθρου 38 παρ. 1 περ. β' του Ν. 4624/2019 (χωρίς δικαίωμα συλλογή, αποθήκευση, οργάνωση, καταχώριση προσωπικών δεδομένων), β) κρατικά απόρρητα, καθώς τότε εφαρμόζονται τα άρθρα 148-149 ΠΚ (Κατασκοπεία), γ) επαγγελματικά ή εμπορικά απόρρητα, υπό την προϋπόθεση ότι ο αποκτών τα χρησιμοποιεί με σκοπό να ανταγωνιστεί την επιχείρηση από την οποία προέρχονται, διότι τότε εφαρμόζεται το άρθρο 16 εδ. β' του Ν. 146/1914 περί αθεμίτου ανταγωνισμού.[32] Επιπροσθέτως, το κενό τιμώρησης καλύπτεται, όταν ο δράστης της αποδοχής είναι και ηθικός αυτουργός στην πράξη με την οποία αποκτώνται παράνομα τα δεδομένα.

Αντιθέτως, κενό παρατηρείται, όταν ο δράστης αποδέχεται παρανόμως κτηθέντα α) επιστημονικά απόρρητα, β) απόρρητα επιχείρησης του δημοσίου τομέα που δεν συνιστούν κρατικά

30. Για τη διάκριση ανάμεσα στον υλικό φορέα αποθήκευσης και τα αποθηκευμένα σε αυτόν δεδομένα, βλ. *Κιούπη,* Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας, Υπερ. 2000, 959 επ., 965-966.

31. Βλ. *Μυλωνόπουλου,* ΠΔ ΕιδΠοιν, [4]2021, σ. 539.

32. Για το ζήτημα αυτό, βλ. *Δανιήλ,* Αθέμιτος Ανταγωνισμός, σε: Παύλου/Σάμιου (εκδ. επιμ.), Ειδικοί Ποινικοί Νόμοι, Ιανουάριος 2012, σ. 64, *Κωνσταντινίδη,* Εγκλήματα των μυημένων και πληροφορημένων από το εσωτερικό μιας επιχειρήσεως ή ενός τομέα οικονομικών δραστηριοτήτων, σε: Ελληνική Εταιρεία Ποινικού Δικαίου, Τα οικονομικά εγκλήματα, Πρακτικά Δ' Συνεδρίου, 1991, σ. 36, *Καϊάφα-Γκμπάντι,* Ποινικό δίκαιο και καταχρήσεις της πληροφορικής, Αρμενόπουλος 2007, 1058 επ., 1074, *Λαζαράτου,* Νεότερες εξελίξεις στην ποινική προστασία των επιχειρηματικών απορρήτων στο δίκαιο του ανταγωνισμού, The Art of Crime, τεύχος Νοεμβρίου 2019.

απόρρητα του άρθρου 149 ΠΚ ή γ) επαγγελματικά ή εμπορικά απόρρητα, εφόσον ο ίδιος δεν έχει σκοπό να τα χρησιμοποιήσει για να ανταγωνιστεί την επιχείρηση από την οποία προέρχονται. Θα ήταν, συνεπώς, ορθότερο να εξεταστεί η θέσπιση αδικήματος αντίστοιχου του άρθρου 202d γερμΠΚ στην ελληνική έννομη τάξη για να καλυφθεί το αξιόποινο της αποδοχής παρανόμως κτηθέντων δεδομένων στις ως άνω περιπτώσεις.