POTAMITISVEKRIS

TMT & PRIVACY

NEWSLETTER

ΑΥΓΟΥΣΤΟΣ, 2024

Περιεχόμενα

EDITORIAL

Καθώς εισερχόμαστε βαθύτερα στην ψηφιακή εποχή, η τεχνητή νοημοσύνη (AI), η προστασία των (προσωπικών) δεδομένων, η κυβερνοασφάλεια, η ρύθμιση των ψηφιακών υπηρεσιών και το δίκαιο της πνευματικής ιδιοκτησίας (IP) έχουν γίνει σημεία αναφοράς. Η ραγδαία εξέλιξη των τεχνολογιών παρουσιάζει πρωτοφανείς ευκαιρίες αλλά και πολύπλοκες προκλήσεις που καθιστούν αναγκαία την επανεξέταση τόσο του υφιστάμενου ρυθμιστικού πλαισίου όσο και του τρόπου λειτουργίας των εταιρειών, που θα πρέπει, πλέον, να επιδιώκουν τον ψηφιακό μετασχηματισμό τους (digital transformation).

Το επόμενο διάστημα θα μας απασχολήσει αρκετά η πρόσφατα ψηφισθείσα η AI Act, η πράξη για την Τεχνητή Νοημοσύνη, που αναμένεται να βοηθήσει μία κάποια οριοθέτηση στον τρόπο που χρησιμοποιούμε αυτοματοποιημένες διαδικασίες ανάλυσης δεδομένων και παραγωγής ενεργειών. Διότι, πράγματι, η ενσωμάτωση της ΤΝ σε διάφορους τομείς θα φέρει επανάσταση στον τρόπο με τον οποίο συλλέγουμε, αναλύουμε και χρησιμοποιούμε δεδομένα αφού τα συστήματα ΤΝ βασίζονται σε μεγάλο βαθμό σε μεγάλα σύνολα δεδομένων για να λειτουργήσουν αποτελεσματικά, εγείροντας σημαντικές ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων.

Οι εταιρείες πρέπει να βρουν μια ισορροπία μεταξύ της χρήσης της καινοτομίας και της προστασίας της ιδιωτικής ζωής αφού η χρήση της ΤΝ αναμένεται διευρυμένη και σε μεγάλο βαθμό ενσωματωμένη σε πολλές λειτουργίες της επιχείρησης, όπως επιλογή προσωπικού, ανάλυση πελατολογίου, συστήματα αυτοματοποιημένων αποφάσεων κλπ. Για το λόγο αυτό οι επιχειρήσεις θα πρέπει να υιοθετήσουν μια ολοκληρωμένη προσέγγιση για τη συμμόρφωση, συμπεριλαμβανομένης της ευαισθητοποίηση του οργανισμού, της διενέργειας αξιολογήσεων κινδύνου, της θέσπισης υπεύθυνων πλαισίων χρήσης ΤΝ και την αυτοματοποίηση των ελέγχων συμμόρφωσης. Η σημαντικότερη διαδικασία που πρέπει να τηρείται με ευλάβεια είναι η δημιουργία και εποπτεία ενός αποτελεσματικού συστήματος διαχείρισης των βάσεων δεδομένων που κάθε οργανισμός κατέχει και επεξεργάζεται (Data Governance). Αν δεν το έκαναν σωστά στα πρώτα στάδια συμμόρφωσης με τον GDPR, θα πρέπει άμεσα να ξαναδούν τις διαδικασίες, τις πολιτικές και τα συστήματα συμμόρφωσης για τα προσωπικά δεδομένα, γιατί η AI Act απαιτεί από τις επιχειρήσεις να εφαρμόζουν ισχυρό πλαίσιο διακυβέρνησης και τεχνικές διασφαλίσεις με απώτερο στόχο τη δημιουργία ενός ασφαλέστερου και ηθικότερου οικοσυστήματος ΤΝ.

Εξίσου σημαντική και η εφαρμογή της DSA (Digital Services Act) η οποία αποτελεί την συνέχεια της Οδηγίας για το ηλεκτρονικό εμπόριο 2000/31/ΕΚ και στοχεύει στη δημιουργία ενός πλαισίου διαφάνειας και λογοδοσίας για τους παρόχους ενδιάμεσων υπηρεσιών, συμπεριλαμβανομένων ιδίως της προστασίας των καταναλωτών, του δικαιώματος της ελευθερίας της έκφρασης και της πληροφόρησης και θεσπίζει υποχρεώσεις δέουσας επιμέλειας για τους παρόχους ενδιάμεσων υπηρεσιών, ώστε να διασφαλίζουν τη διαφάνεια και την ασφάλεια στο ψηφιακό περιβάλλον.

Περαιτέρω, στην χρονιά των Ολυμπιακών Αγώνων, η γαλλική αρχή προστασίας των προσωπικών δεδομένων CNIL (μία από τις πιο ενεργείς αρχές στην Ε.Ε.) συνέδραμε ενεργά στη διασφάλιση της συμμόρφωσης των φορέων εκμετάλλευσης που εφαρμόζουν τα συστήματα για την ασφάλεια των αγώνων, των αθλητών και των επισκεπτών,

ενώ παράλληλα, εξέδωσε Q&A με σκοπό να αναλύσει τον τρόπο λειτουργίας τους καθώς και τα όρια στην επίβλεψη ιδιωτικών και δημόσιων χώρων με κάμερες ή άλλα συστήματα ασφαλείας.

Τέλος, μία πολύ σημαντική απόφαση του Γενικού Δικαστηρίου της Ε.Ε. μας υπενθύμισε ότι τα σήματα φήμης υπόκεινται στην απαίτηση της ουσιαστικής χρήσης και μπορούν να ανακληθούν εάν ο δικαιούχος δεν προσκομίσει επαρκή αποδεικτικά στοιχεία για κάθε ειδικότερη κατηγορία προϊόντων και υπηρεσιών, που προστατεύονται από το σήμα του.

Στο παρόν newsletter μας επιχειρούμε μία πρώτη ενημέρωση για τα σημαντικότερα ζητήματα που αφορούν κάθε σύγχρονη επιχείρηση και πιστεύουμε ότι αποτελεί ένα ωραίο ανάγνωσμα είτε πριν είτε κατά την διάρκεια των διακοπών σας!

Σπ. Τάσσης
Εταίρος (TMT&Privacy)

Ο Κανονισμός (ΕΕ) 2022/2065: Digital Services Act (Πράξη για τις ψηφιακές υπηρεσίες)

Εισαγωγή στο πεδίο

Η Πράξη για τις Ψηφιακές Υπηρεσίες[1] (Digital Services Act, εφεξής ο «DSA») αποσκοπεί στη ρύθμιση της λειτουργίας των διαδικτυακών παρόχων ενδιάμεσων υπηρεσιών. Ο DSA εφαρμόζεται ήδη από την 17η Φεβρουαρίου 2024 σε ένα ευρύ φάσμα παρόχων ενδιάμεσων υπηρεσιών, όπως είναι τα marketplaces, οι μηχανές κράτησης καταλυμάτων, οι υπηρεσίες φιλοξενίας ιστοσελίδων, οι υπηρεσίες υπολογιστικού νέφους, τα μέσα κοινωνικής δικτύωσης κ.ά.

Ο DSA, με γνώμονα την προάσπιση και τη θωράκιση των θεμελιωδών δικαιωμάτων των χρηστών του διαδικτύου, συμπεριλαμβανομένων ιδίως του δικαιώματος προστασίας των καταναλωτών, του δικαιώματος της ελευθερίας της έκφρασης και της πληροφόρησης, στοχεύει στη δημιουργία ενός πλαισίου διαφάνειας και λογοδοσίας για τους παρόχους ενδιάμεσων υπηρεσιών, ώστε να περιορίζεται η διάδοση του παράνομου περιεχομένου στο διαδίκτυο[2] . Τα κύρια σημεία αυτού του πλαισίου περιλαμβάνουν τα εξής:

Διατήρηση του Κανόνα της Μη Επιβολής Γενικής Υποχρέωσης Παρακολούθησης:

Ο DSA διατηρεί τον κανόνα της μη επιβολής γενικής υποχρέωσης παρακολούθησης[3] , όπως θεσπίστηκε με την Οδηγία 2000/31 για το ηλεκτρονικό εμπόριο[4] . Οι πάροχοι ενδιάμεσων υπηρεσιών δεν υποχρεούνται να αναζητούν ενεργά γεγονότα που μπορεί να αφορούν παράνομη δραστηριότητα και δεν είναι υποχρεωμένοι να λαμβάνουν εκ των προτέρων μέτρα για την αποτροπή του παράνομου περιεχομένου. Η Οδηγία του 2002 δεν καταργείται, αλλά εξειδικεύεται, υπό το πρίσμα των καινοτόμων ψηφιακών υπηρεσιών οι οποίες έχουν αναπτυχθεί, ανάγκη που κρίθηκε επιβεβλημένη, προκειμένου να διασφαλιστεί ότι το σύγχρονο επιγραμμικό περιβάλλον χαρακτηρίζεται από όρους ασφάλειας, προβλεψιμότητας και αξιοπιστίας.

Υποχρεώσεις Δέουσας Επιμέλειας:

Ο DSA θεσπίζει υποχρεώσεις δέουσας επιμέλειας για τους παρόχους ενδιάμεσων υπηρεσιών, ώστε να διασφαλίζουν τη διαφάνεια και την ασφάλεια στο ψηφιακό περιβάλλον. Οι υποχρεώσεις περιλαμβάνουν ενδεικτικά: συμπερίληψη στους όρους και προϋποθέσεις του παρόχου πληροφοριών σχετικά με τις πολιτικές και διαδικασίες που ο πάροχος εφαρμόζει για τον έλεγχο του περιερχομένου και τυχόν περιορισμούς τους οποίους επιβάλλει σε σχέση με τη χρήση της παρεχόμενης υπηρεσίας, θέσπιση μηχανισμών ειδοποίησης σχετικά με εικαζόμενο παράνομο περιεχόμενο και ανάληψης δράσης, αναφορά υπονοιών τέλεσης ποινικών αδικημάτων στις αρχές επιβολής του νόμου, δημοσίευση εκθέσεων σχετικά με τη διαφάνεια.

---

[1] Διαθέσιμη εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32022R2065

[2] Περισσότερες πληροφορίες για τον DSA από την Ευρωπαϊκή Επιτροπή διαθέσιμες εδώ: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_el

[3] Άρθρο 8 - Μη επιβολή γενικής υποχρέωσης παρακολούθησης ή ενεργητικής αναζήτησης γεγονότων: Δεν επιβάλλεται στους παρόχους ενδιάμεσων υπηρεσιών γενική υποχρέωση παρακολούθησης των πληροφοριών που μεταδίδουν ή αποθηκεύουν, ούτε γενική υποχρέωση ενεργητικής αναζήτησης γεγονότων ή περιστάσεων που υποδηλώνουν παράνομη δραστηριότητα.

[4] Διαθέσιμη εδώ: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32000L0031

Κλιμάκωση Υποχρεώσεων:

Οι βασικές υποχρεώσεις ισχύουν για όλους τους παρόχους ενδιάμεσων υπηρεσιών και κλιμακώνονται, ανάλογα με το ρόλο του παρόχου ως: πάροχος υπηρεσιών φιλοξενίας, πάροχος επιγραμμικής πλατφόρμας, πάροχος επιγραμμικής πλατφόρμας που δίνει στους καταναλωτές τη δυνατότητα να συνάπτουν εξ αποστάσεως συμβάσεις με εμπόρους και πάροχος πολύ μεγάλης επιγραμμικής πλατφόρμας και πολύ μεγάλης επιγραμμικής μηχανής αναζήτησης, ενώ πολλές από τις υποχρεώσεις δεν τυγχάνουν εφαρμογής σε παρόχους ενδιάμεσων υπηρεσιών οι οποίοι θεωρούνται πολύ μικρές[5] ή μικρές επιχειρήσεις[6].

Εθνικό νομοθετικό πλαίσιο

Τον Απρίλιο του 2024, δημοσιεύθηκε ο νόμος 5099/2024 για την εφαρμογή του DSA, ορίζοντας τις αρμόδιες αρχές για την επιβολή του στην Ελλάδα. Συγκεκριμένα: Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) ορίστηκε ως ο Συντονιστής Ψηφιακών Υπηρεσιών, ενώ το Εθνικό Συμβούλιο Ραδιοτηλεόρασης (ΕΣΡ) και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) ορίστηκαν ως οι αρμόδιες αρχές για την επίβλεψη των παρόχων.

Η ΕΕΤΤ ήδη ασκεί ενεργά τις εξουσίες και αρμοδιότητες που απονέμονται στον Συντονιστή Ψηφιακών Υπηρεσιών από τον DSA και τον ελληνικό νόμο και έχει ήδη προβεί:

- στην έκδοση οδηγιών[7] όσον αφορά την εγγραφή των παρόχων επιγραμμικών πλατφορμών στη «Βάση Δεδομένων Διαφάνειας» της Ευρωπαϊκής Επιτροπής, υποχρέωση που πηγάζει από το άρθρο 24 παρ. 5 του DSA
- στη δημοσίευση Κανονισμού[8] Λειτουργίας Μητρώου Παρόχων Ενδιάμεσων Υπηρεσιών συμπεριλαμβανομένων των Υπηρεσιών Φιλοξενίας, στο οποίο (Μητρώο) οι πάροχοι ενδιάμεσων υπηρεσιών οφείλουν να πραγματοποιήσουν την εγγραφή τους
- στη δημοσίευση της διαδικασίας για την αναγνώριση της ιδιότητας της «Αξιόπιστης πηγής επισήμανσης παράνομου περιεχομένου (trusted flagger)» σε ενδιαφερόμενους φορείς που εδρεύουν στην Ελλάδα, στο πλαίσιο του DSA, υποχρέωση που πηγάζει από το Άρθρο 22 του DSA

Αποτίμηση του Κανονισμού

Είναι κρίσιμο για τις επιχειρήσεις που λειτουργούν ως πάροχοι ενδιάμεσων υπηρεσιών να προσαρμοστούν στο νέο πλαίσιο υποχρεώσεων που έχει θεσπίσει ο DSA, παρακολουθώντας τις αποφάσεις που εκδίδονται από τις αρμόδιες εθνικές αρχές. Η έγκαιρη και ορθή προσαρμογή στις κανονιστικές απαιτήσεις συνεπάγεται την ενίσχυση της προστασίας των καταναλωτών, καθιστώντας την εμπειρία των χρηστών του διαδικτύου ασφαλέστερη.

---

[5] Όπως ορίζονται στη σύσταση 2003/361/ΕΚ: «Στην κατηγορία των ΜΜΕ, ως πολύ μικρή επιχείρηση ορίζεται η επιχείρηση η οποία απασχολεί λιγότερους από δέκα εργαζομένους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 2 εκατομμύρια ευρώ.»

[6] Όπως ορίζονται στη σύσταση 2003/361/ΕΚ: «Στην κατηγορία των ΜΜΕ, ως μικρή επιχείρηση ορίζεται η επιχείρηση η οποία απασχολεί λιγότερους από 50 εργαζομένους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 10 εκατομμύρια ευρώ.»

[7] Διαθέσιμες εδώ: https://www.greekecommerce.gr/wp-content/uploads/2024/04/%CE%95%CE%B3%CE%B3%CF%81%CE%B1%CF%86%CE%B7%CC%81-%CF%83%CE%B5-%CE%92%CE%94_%CE%94%CE%B9%CE%B1%CF%86%CE%B1%CC%81%CE%BD%CE%B5%CE%B9%CE%B1%CF%82.pdf

[8] ΦΕΚ 4299/Β/23-07-2024, διαθέσιμο εδώ: https://www.eett.gr/wp-content/uploads/2024/07/%CE%91%CE%A0.1119-002.pdf

Χρήση λογισμικού για έλεγχο λογοκλοπής στο χώρο των Πανεπιστημίων

Ένα από τα πιο καίρια ζητήματα που απασχολούν το χώρο της ακαδημαϊκής κοινότητας είναι εκείνο της λογοκλοπής και των επιτακτικών μέτρων για την αντιμετώπισή της.

Στο σημείο αυτό, κρίσιμο φαίνεται να είναι το ερώτημα :

Έχουν το δικαίωμα τα πανεπιστήμια να χρησιμοποιήσουν ειδικό λογισμικό για τον έλεγχο περιπτώσεων λογοκλοπής σε εργασίες φοιτητών και να διαβιβάσουν δεδομένα τους στην εταιρεία που το διαχειρίζεται; Ή με άλλα λόγια, είναι νόμιμη η επεξεργασία αυτή των δεδομένων;

Αφορμή για την απάντηση του ανωτέρω ερωτήματος στάθηκε καταγγελία φοιτήτριας στην αρχή προστασίας δεδομένων της Βόρειας Ρηνανίας-Βεστφαλίας (LDI/NRW). Πιο συγκεκριμένα, η φοιτήτρια έκανε λόγο για παράνομη επεξεργασία των προσωπικών της δεδομένων από Πανεπιστήμιο μέσω της χρήσης ειδικού λογισμικού για έλεγχο λογοκλοπής.

Η γερμανική εποπτική αρχή για το συγκεκριμένο ζήτημα επισημαίνει πως για να είναι νόμιμη αυτή η επεξεργασία των δεδομένων θα πρέπει να τηρούνται ορισμένες προϋποθέσεις.

Αρχικά, η επεξεργασία θα πρέπει να γίνεται με βάση τις προϋποθέσεις του άρθρου 5 παρ. 1 εδάφιο ε του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) στο πλαίσιο εκτέλεσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον, σύμφωνα με το οποίο : «Τα προσωπικά δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομέ να προσωπικού χαρακτήρα μπορούν να αποθ ηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της περιόδου αποθήκευσης»)» και υπό την προϋπόθεση ότι η χρήση λογισμικού προβλέπεται στους κανονισμούς του Πανεπιστημίου που ρυθμίζουν τη διαδικασία διεξαγωγής των εξετάσεων και την εκπόνηση εργασιών.

Σημειώνεται πως η γερμανική αρχή αποκλείει οποιαδήποτε πιθανότητα επίκλησης συγκατάθεσης ως νομική βάση για την εν λόγω επεξεργασία, καθώς όχι μόνο εντοπίζεται σχέση ανισότητας ανάμεσα στα πανεπιστήμια και στους φοιτητές, αλλά και μία συγκατάθεση που δίνεται υπό των φόβο των συνεπειών στην ακαδημαϊκή πορεία όσων την αρνηθούν μόνο ελεύθερη δεν θεωρείται.

Μια δεύτερη προϋπόθεση για να είναι νόμιμη η επεξεργασία, αποτελεί η ψευδωνυμοποίηση των προσωπικών δεδομένων των φοιτητών που θα υποβληθούν σε έλεγχο. Τα πανεπιστήμια αφενός θα πρέπει να διασφαλίζουν ότι τα αποτελέσματα του ελέγχου για λογοκλοπή θα μπορούν να αντιστοιχιστούν με συγκεκριμένο φοιτητή και να είναι έγκυρα, αφετέρου κανένας εξωτερικός πάροχος που διαχειρίζεται τα ειδικά αυτά λογισμικά δεν χρειάζεται να γνωρίζει τα αναγνωριστικά στοιχεία του κάθε φοιτητή.

Επιπλέον, τα πανεπιστήμια, για να εξασφαλίσουν τη νομιμότητα της επεξεργασίας, οφείλουν να διαγράφουν από τα συστήματα τους τις εργασίες των φοιτητών μετά το πέρας της διαδικασίας ελέγχου, καθώς και να τους ενημερώνουν πως θα γίνει χρήση λογισμικού κατά της λογοκλοπής και κατ' επέκταση επεξεργασία των δεδομένων τους.

Στο ερώτημα, λοιπόν, εάν τα πανεπιστήμια μπορούν να κάνουν χρήση ειδικού λογισμικού για τον έλεγχο της λογοκλοπής, η αρχή προστασίας δεδομένων της Βόρειας Ρηνανίας-Βεστφαλίας (LDI/NRW) απαντά καταρχήν θετικά, θέτει όμως και συγκεκριμένες προϋποθέσεις για τη νομιμότητα του εγχειρήματος.

Υποθέσεις Hermes και Chanel -απειλή για τα σήματα φήμης

Δυο υποθέσεις κατά τις οποίες μεγαθήρια του εμπορίου και της μόδας «ηττήθηκαν» από μικρότερες εταιρείες, που δύναται πλέον να χρησιμοποιούν τα εμπορικά σήματα της Hermes και της Chanel, έλαβαν χώρα τους τελευταίους μήνες.

Σε ένα μικρό βιβλιοπωλείο στην Τουρκία και ειδικότερα στη Σμύρνη επετράπη η χρήση του εμπορικού σήματος "Hermes" ανατρέποντας εν μέρει, με νέα δικαστική απόφαση από τα δικαστήρια της Άγκυρας, την απόφαση του γραφείου πνευματικών δικαιωμάτων της Τουρκίας (TurkPatent) η οποία εμπόδιζε οποιαδήποτε εταιρεία εκτός από την Hermes Paris να χρησιμοποιεί τον όρο «Hermes».

Ο ισχυρισμός του βιβλιοπωλείου βασίστηκε στο γεγονός ότι ο όρος «Hermes» προέρχεται από το θεό της ελληνικής μυθολογίας που συνδέεται στενά με την αρχαία ιστορία της Σμύρνης και τις ακτές του Αιγαίου, αποτελώντας πολιτιστική κληρονομία της ανθρωπότητας, η οποία δεν δύναται να ανήκει και να μονοπωλείται από μια εταιρεία.

Η υπόθεση ξεκίνησε το 2021, όταν ο ιδιοκτήτης του βιβλιοπωλείου επεχείρησε να κατοχυρώσει το εμπορικό σήμα για το 15 ετών βιβλιοπωλείο του και η γαλλική εταιρεία ισχυριζόμενη ομοιότητα και κίνδυνο σύγχυσης προσπάθησε να τον εμποδίσει. Η απόφαση του δικαστηρίου δεν έχει ακόμη δημοσιευθεί αλλά παρουσιάζει εξαιρετικό ενδιαφέρον καθώς θα δημιουργήσει προηγούμενο στη νομολογία αναφορικά με τους όρους πολιτιστικής κληρονομιάς και τα εμπορικά σήματα φήμης.

Μια ακόμα ανατροπή κατέστησε σαφές ότι κανένα εμπορικό σήμα δεν είναι απρόσβλητο στις νομικές διαμάχες. Το Γραφείο Πνευματικής Ιδιοκτησίας της Ευρωπαϊκής Ένωσης (EUIPO) απέρριψε την ανακοπή της εταιρείας Chanel για την ομοιότητα του εμπορικού σήματος M5 με το γνωστό άρωμα Chanel N°5.

Μια μικρή σλοβενική εταιρεία, η Simb D.O.O., καταχωρώντας το εμπορικό σήμα M5, επιχείρησε να εισέλθει δυναμικά στην αγορά καλλυντικών με ένα λογότυπο που περιλαμβάνει ένα στυλιζαρισμένο 5 γύρω από το γράμμα M. Η Chanel, αντιλαμβανόμενη την απειλή, αντέδρασε γρήγορα ασκώντας ανακοπή. Βασικός ισχυρισμός ήταν ο κίνδυνος σύγχυσης, λόγω της ομοιότητας και της σημασίας που έχει αποκτήσει ο αριθμός 5 στη συνείδηση του καταναλωτικού κοινού προσκομίζοντας μάλιστα διαφημιστικά φυλλάδια, φωτογραφίες από βιτρίνες καταστημάτων και αντίγραφα σελίδων της Wikipedia.

Επίσης επεσήμανε τον κίνδυνο το νέο σήμα να παραπλανήσει τους καταναλωτές και να αποδυναμώσει την εικόνα και τη διακριτική δύναμη του εμπορικού σήματος της Chanel αποκτώντας μάλιστα αθέμιτο πλεονέκτημα στην αγορά λόγω της θετικής εικόνας της Chanel η οποία έχει δημιουργηθεί με μεγάλες επενδύσεις και ποικίλες εμπορικές πρακτικές της εταιρείας.

Το EUIPO δεν πείστηκε και στις 17 Ιουνίου με την απόφασή του επεσήμανε ότι δε συντρέχει κίνδυνος σύγχυσης μεταξύ των δύο εμπορικών σημάτων. Σύμφωνα με το EUIPO, το λογότυπο M5, δεν παραβιάζει τα δικαιώματα της Chanel επί του N°5 και τα στοιχεία που προσκομίστηκαν δεν ήταν επαρκή. Καθοριστικό ρόλο έπαιξε η απουσία ποσοτικών στοιχείων αναφορικά με τις πωλήσεις και την έκθεση του κοινού στο εμπορικό σήμα N°5. Χωρίς αυτά τα στοιχεία, δε μπορεί να αποδειχθεί ότι οι καταναλωτές θα συνέδεαν αυτόματα τον αριθμό 5 με το σήμα της Chanel.

Η απόφαση αυτή αποκαλύπτει τις δυσκολίες που αντιμετωπίζουν τα εμπορικά σήματα πολυτελείας στην προστασία της εικόνας τους, αυξάνοντας παράλληλα τον κίνδυνο από μικρές εταιρείες που θα θελήσουν να επωφεληθούν από τη φήμη και τη θετική εικόνα των διάσημων εταιρειών.

Τα «εμπορικά σήματα φήμης», τα γραφεία εμπορικών σημάτων και κατ' επέκταση τα δικαστήρια θα πρέπει να επανεξετάσουν τις δομές της αγοράς και βρουν την κατάλληλη ισορροπία ανάμεσα στην προστασία των εμπορικών σημάτων και την εξασφάλιση του θεμιτού ανταγωνισμού.

Η CNIL ως πρόμαχος των προσωπικών δεδομένων στους Ολυμπιακούς και Παραολυμπιακούς Αγώνες 2024

Αυτή την περίοδο όλα τα βλέμματα είναι στραμμένα στο Παρίσι για τη διεξαγωγή των Ολυμπιακών και Παραολυμπιακών Αγώνων (εφεξής οι «Αγώνες»). Τα μέτρα ασφαλείας στην «Πόλη του Φωτός» είναι δρακόντεια στη σκιά του φόβου για ένα – ακόμη - τρομοκρατικό χτύπημα, με τους μόνιμους κατοίκους να αναφέρουν ότι «δεν είναι το Παρίσι αυτό που βλέπετε[9]» . Αρκετά από τα ληφθέντα μέτρα ασφαλείας παρεμβαίνουν προδήλως στην ιδιωτική σφαίρα και τις ατομικές ελευθερίες των επισκεπτών όσο και των μονίμων κατοίκων της πόλης, γεγονός που κινητοποίησε τη Γαλλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Commission Nationale de l'Informatique et des Libertés – «CNIL») στο να προβεί από το 2023 σε γνωμοδοτήσεις επί των σχετικών νομοθετικών ρυθμίσεων, καθώς και να εκδίδει μέχρι και σήμερα σχετικές ανακοινώσεις/κατευθύνσεις προς το κοινό.

Ο γαλλικός Νόμος της 19ης Μαΐου 2023 σχετικά με τους Αγώνες[10] (εφεξής ο «Γαλλικός Νόμος») προβλέπει την πειραματική εφαρμογή ορισμένων ειδικών συστημάτων ασφαλείας, μεταξύ των οποίων: α) τη χρήση «ενισχυμένου» συστήματος καμερών (caméras «augmentées») που ενσωματώνει πρόγραμμα λογισμικού αυτόματης ανάλυσης εικόνας και μπορεί να ανιχνεύσει συγκεκριμένα αντικείμενα[11] , β) την υποχρεωτική έκδοση δελτίου με κωδικό QR που θα επιτρέπει στους θεατές (επισκέπτες/μόνιμους κατοίκους) να έχουν πρόσβαση σε ορισμένες περιοχές του Παρισιού και των γύρω διαμερισμάτων[12] , και γ) τη χρήση σαρωτή σώματος που ελέγχει την απουσία απαγορευμένων αντικειμένων σε ορισμένους χώρους που θα διεξαχθούν Αγώνες με σκοπό τη διευκόλυνση και διασφάλιση της πρόσβασης του κοινού. Ο εν λόγω πειραματισμός θα λήξει την 31η Μαρτίου 2025, οπότε και τα προαναφερθέντα συστήματα δεν θα μπορούν πλέον να χρησιμοποιηθούν, εκτός εάν παραταθεί η χρήση αυτών με νέο ειδικό Νόμο.

Η CNIL συνέδραμε ενεργά στη διασφάλιση της συμμόρφωσης των φορέων εκμετάλλευσης που εφαρμόζουν τα προαναφερθέντα συστήματα[13] , ενώ παράλληλα, εξέδωσε Q&A[14] με σκοπό να ρίξει

---

[9] Βλ. Σπυριδούλα Σπανέα (2024), «Δεν είναι το Παρίσι αυτό που βλέπετε», λένε οι κάτοικοι», Η ΚΑΘΗΜΕΡΙΝΗ. https://www.kathimerini.gr/world/563146018/den-einai-to-parisi-ayto-poy-vlepete-lene-oi-katoikoi/

[10] https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000046777392/

[11] Για παράδειγμα, παρουσία εγκαταλελειμμένων αντικειμένων, παρουσία ή χρήση όπλων, η διέλευση ή η παρουσία ατόμου ή οχήματος σε απαγορευμένη ή ευαίσθητη περιοχή, υπερβολικά υψηλή πυκνότητα ανθρώπων, κ.λπ.

[12] Η περίμετρος προστασίας «SILT» (Sécurité Intérieure et Lutte contre le Terrorisme), εντός της οποίας θα ρυθμίζεται η κυκλοφορία οχημάτων και πεζών και θα διενεργούνται έλεγχοι ασφαλείας, και η «κόκκινη» περίμετρος προστασίας, όπου θα περιορίζεται μόνο η οδική κυκλοφορία. Βλ. La Préfecture de Police de Paris (2024), Les périmètres de sécurité autour des sites olympiques et paralympiques https://www.prefecturedepolice.interieur.gouv.fr/mission/des-jeux-securises-pour-tous/les-perimetres-de-securite-autour-des-sites-olympiques-et-paralympiques

[13] Η CNIL παρακολούθησε την πρώτη δοκιμή «ενισχυμένου» συστήματος καμερών σε πραγματικές συνθήκες που διοργάνωσε η αστυνομία του Παρισιού κατά τη διάρκεια της συναυλίας των Depeche Mode στο Accor Arena στο Παρίσι στις 5/3/24: η συσκευή ήταν σε θέση να ελέγχει την πυκνότητα του πλήθους, να εντοπίζει άτομα ή οχήματα που περνούν σε απαγορευμένες περιοχές, να εντοπίζει την έναρξη πυρκαγιάς κ.λπ. Βλ. Commission Nationale de l'Informatique et des Libertés (2024), JOP 2024: les questions-réponses de la CNIL sur votre vie privée et vos libertés. Διαθέσιμο στο: https://www.cnil.fr/fr/jop-2024-les-questions-reponses-de-la-cnil.

[14] Βλ. Commission Nationale de l'Informatique et des Libertés (2024), JOP 2024: les questions-réponses de la CNIL sur votre vie privée et vos libertés, ο.π.

περισσότερο φως στην υλοποίηση αυτών. Επιγραμματικά, η CNIL έχει επισημάνει τα εξής:

Για το «ενισχυμένο» σύστημα καμερών

Το «ενισχυμένο» σύστημα καμερών μπορεί να χρησιμοποιηθεί μόνο για την ασφάλεια εκδηλώσεων μεγάλης κλίμακας (όπως η τελετή έναρξης των Αγώνων), οι οποίες είναι ιδιαίτερα εκτεθειμένες στον κίνδυνο τρομοκρατικών ενεργειών ή σοβαρών απειλών κατά της ατομικής και συλλογικής ασφάλειας. Συγκεκριμένα, οι συσκευές αυτές μπορούν να χρησιμοποιηθούν μόνο στον χώρο της εκδήλωσης, στην περιοχή της εκδήλωσης και στα μέσα μαζικής μεταφοράς, δηλαδή σε σταθερές κάμερες που υπάρχουν ήδη στους δρόμους, σε σιδηροδρομικούς σταθμούς ή εντός των εγκαταστάσεων του μετρό και του προαστιακού σιδηροδρόμου, αλλά και σε μη επανδρωμένα αεροσκάφη.

Τα εν λόγω συστήματα επιτρέπουν την αναφορά των καταστάσεων που αναφέρονται παραπάνω σε εξουσιοδοτημένους πράκτορες, οι οποίοι ελέγχουν τις ειδοποιήσεις για να τις επικυρώσουν ή όχι. Στη συνέχεια, αποφασίζουν ποια ενέργεια πρέπει να αναλάβουν και, ιδίως, εάν είναι απαραίτητο να ειδοποιήσουν τις αρμόδιες υπηρεσίες. Συνεπώς, τα συμβάντα που εντοπίζονται υπόκεινται πάντοτε σε ανθρώπινη ανάλυση πριν από τη λήψη οποιασδήποτε ενέργειας. Συνεπώς, ένας επισκέπτης/μόνιμος κάτοικος δεν μπορεί να διωχθεί μόνο βάσει των αλγοριθμικών διαδικασιών του «ενισχυμένου» συστήματος καμερών.

Το «ενισχυμένο» σύστημα καμερών που θα χρησιμοποιηθεί κατά τη διάρκεια των Αγώνων δεν θα εφαρμόζει αναγνώριση προσώπου, καθώς βάσει του Γαλλικού Νόμου αποκλείεται ρητά η χρήση οποιουδήποτε συστήματος βιομετρικής ταυτοποίησης ή τεχνικών αναγνώρισης προσώπου.

Ως προς το χρόνο τήρησης των συλλεγόμενων δεδομένων, τα δεδομένα που συλλέγονται από το «ενισχυμένο» σύστημα καμερών θα διατηρηθούν για μέγιστο χρονικό διάστημα ενός έτους μετά την καταγραφή.

Για το δελτίο με κωδικό QR

Για τη χορήγηση του ειδικού δελτίου, οι γαλλικές Αρχές θα συλλέξουν προσωπικά δεδομένα του επισκέπτη/μόνιμου κάτοικου, μεταξύ των οποίων ονοματεπώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμό τηλεφώνου, φωτογραφία, απόδειξη της πρόσβασης στη ζώνη (απόδειξη κατοικίας ή απόδειξη εργασίας), αριθμός και αντίγραφο δελτίου ταυτότητας, άδειας οδήγησης, διαβατηρίου ή άδειας διαμονής, ημερομηνίες και ώρες εισόδου και εξόδου από την ασφαλή ζώνη, αντίγραφο της άδειας κυκλοφορίας (για τα οχήματα). Όλα αυτά τα δεδομένα διατηρούνται για τρεις μήνες μετά το τέλος της εκάστοτε εκδήλωσης, εκτός από το αντίγραφο της ταυτότητας, της άδειας οδήγησης, του διαβατηρίου ή της άδειας διαμονής, το οποίο θα διατηρηθεί μόνο μέχρι να ετοιμαστεί και να αποσταλεί στον επισκέπτη/μόνιμο κάτοικο το δελτίο με κωδικό QR.

Για το σαρωτή σώματος

Το εν λόγω σύστημα θα θολώνει το εκάστοτε πρόσωπο του επισκέπτη/μόνιμου κάτοικου, ενώ δεν θα είναι δυνατή η ταυτόχρονη προβολή της ταυτότητας του επισκέπτη/μόνιμου κατοίκου και της εικόνας που παράγει ο σαρωτής. Ο κάθε επισκέπτης/μόνιμος κάτοικος (ως υποκείμενο δεδομένων) θα πρέπει να δώσει προηγουμένως τη ρητή συγκατάθεσή του. Σε περίπτωση άρνησής του, ενδέχεται να υποβληθεί σε άλλου είδους έλεγχο, όπως χειροκίνητο έλεγχο. Σε κάθε περίπτωση, οι εικόνες του σαρωτή σώματος δεν θα καταγράφονται ούτε θα αποθηκεύονται σε βάσεις δεδομένων.

Τέλος, μέσω του πρόσφατου Q&A η CNIL ενημερώνει το κοινό για το πως μπορεί να ασκήσει τα δικαιώματά του ως υποκείμενο δεδομένων, ήτοι το δικαίωμά πρόσβασης, διόρθωσης, περιορισμού ή διαγραφής των προσωπικών του δεδομένων, παραθέτοντας συνάμα τους τρόπους επικοινωνίας με τους αρμόδιους φορείς (είτε μέσω διευθύνσεων ηλεκτρονικού ταχυδρομείου είτε ταχυδρομικώς)[15].

[15] Βλ. Commission Nationale de l'Informatique et des Libertés (2024), JOP 2024: les questions-réponses de la CNIL sur votre vie privée et vos libertés, ο.π.

McDonald's μερική ακύρωση ΕΕ σήματος BIG MAC

Σύμφωνα με την πρόσφατη απόφαση του Γενικού Δικαστηρίου σχετικά με το σήμα «BIG MAC» της McDonald's (υπόθεση T-58/23[16]), τα σήματα φήμης υπόκεινται στην απαίτηση της ουσιαστικής χρήσης και μπορούν να ανακληθούν εάν ο δικαιούχος δεν προσκομίσει επαρκή αποδεικτικά στοιχεία για κάθε ειδικότερη κατηγορία προϊόντων και υπηρεσιών, που προστατεύονται από το σήμα του. Η προσκόμιση διαφημιστικών αφισών, μενού και φωτογραφιών από τηλεοπτικά διαφημιστικά σποτ εκ μέρους της McDonald's κρίθηκε από το Γενικό Δικαστήριο ανεπαρκής για την απόδειξη της ουσιαστικής χρήσης και της έκτασης αυτής, ιδίως αναφορικά με τον όγκο των πωλήσεων, τη διάρκεια της περιόδου χρήσης και τη συχνότητα της χρήσης.

Ειδικότερα, στις 11 Απριλίου 2017, η εταιρεία Supermac's (Holdings) Ltd (Supermac's) υπέβαλε αίτηση έκπτωσης της McDonald's από το ευρωπαϊκό εμπορικό της σήμα με αριθμό 000062638 «BIG MAC», το οποίο καταχωρίστηκε την 1η Απριλίου 1996 για προϊόντα και υπηρεσίες των κλάσεων 29, 30 και 42. Με την προσφυγή της η Supermac's, επικαλούμενη τις σχετικές διατάξεις του άρθρου 58 παράγραφος 1 στοιχείο α' του Ευρωπαϊκού Κανονισμού (ΕΕ) 2017/1001 της 14ης Ιουνίου 2017 για το σήμα της Ευρωπαϊκής Ένωσης (EUTMR), αιτείτο την έκπτωση του σήματος «BIG MAC», για ορισμένα προϊόντα και υπηρεσίες, λόγω μη χρήσης στην Ευρωπαϊκή Ένωση σε σχέση με τα εν λόγω προϊόντα και υπηρεσίες σε διάστημα συνεχούς περιόδου πέντε ετών.

Το Γραφείο Διανοητικής Ιδιοκτησίας της Ευρωπαϊκής Ένωσης (EUIPO) προχώρησε στην ακύρωση του σήματος για όλα τα προϊόντα και τις υπηρεσίες.

Κατόπιν προσφυγής, το τμήμα προσφυγών του EUIPO («BoA») ακύρωσε εν μέρει την απόφαση του EUIPO και διαπίστωσε ότι η McDonald's απέδειξε πραγματική χρήση του επίμαχου σήματος «BIG MAC», μεταξύ άλλων, για τα τρόφιμα που παρασκευάζονται από κρέας και πουλερικά και τα σάντουιτς με κρέας και κοτόπουλο, καθώς και όσον αφορά τις υπηρεσίες που παρέχονται ή συνδέονται με τη λειτουργία εστιατορίων και άλλων εγκαταστάσεων ή εγκαταστάσεων που ασχολούνται με την παροχή φαγητών και ποτών παρασκευασμένων για κατανάλωση και για εγκαταστάσεις drive-through, καθώς και για τις υπηρεσίες παρασκευής τροφίμων για μεταφορά. Εν συνεχεία Το Γενικό Δικαστήριο έκανε εν μέρει δεκτή την προσφυγή της εταιρείας Supermac's και ακύρωσε την απόφαση του τμήματος προσφυγών του EUIPO, αναφορικά με τα «σάντουιτς με κοτόπουλο» των κλάσεων 29 και 30, τα «τρόφιμα που παρασκευάζονται από προϊόντα πουλερικών» της κλάσης 29 και τις υπηρεσίες της κλάσης 42, ενώ το επίμαχο εμπορικό σήμα εξακολουθεί να ισχύει για τις ευρύτερες κατηγορίες προϊόντων «βρώσιμα σάντουιτς», «σάντουιτς με κρέας» και «τρόφιμα που παρασκευάζονται από προϊόντα κρέατος».

Από την παραπάνω απόφαση είναι εμφανές ότι η επιλογή ευρύτερων κατηγοριών προϊόντων και υπηρεσιών για προστασία από ευρωπαϊκά εμπορικά σήματα, εξασφαλίζει περισσότερη ασφάλεια και μελλοντική ευελιξία στους δικαιούχους εμπορικών σημάτων και παρέχει δικλείδες ασφαλείας για την

---

[16] Judgement of 5 June 2024, of the General Court (Sixth Chamber) Supermac's (Holdings) Ltd v. European Union Intellectual Property Office (EUIPO), case T-58/23, διαθέσιμή εδώ: https://curia.europa.eu/juris/document/document.jsf;jsessionid=D91371C3643028D30A6AC54AC4872CC3?text=&docid=286812&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4952871

ενίσχυση των επιχειρημάτων και την απόδειξη ουσιαστικής χρήσης αυτών[17] . Με άλλα λόγια, κατά τη διαδικασία καταχώρισης κλάσεων προϊόντων και υπηρεσιών ενός εμπορικού σήματος, θα πρέπει να δίνεται ιδιαίτερη σημασία στην επιλογή όσο το δυνατόν γενικότερων κατηγοριών και διατυπώσεων, ώστε να καλύπτονται τυχόν ειδικότερες κατηγορίες αυτών και να περιορίζεται ο κίνδυνος επίκλησης από τρίτους λόγων έκπτωσης λόγω μη συνεχούς πενταετούς χρήσης.

[17] Βλ. Pemsel, Marcel , «BIG MAC, General Court, Marcel Pemsel, McDonald's» June 22, 2024, The IPKat online blogspot, διαθέσιμο εδώ: https://ipkitten.blogspot.com/2024/06/mcdonalds-big-mac-partially-cancelled.html

Αποτελεί η βιντεοεπιτήρηση συλλογή και επεξεργασία προσωπικών δεδομένων απευθείας από το υποκείμενο σύμφωνα με το άρθρο 13 του ΓΚΠΔ;

Απαρχή κάθε επεξεργασίας προσωπικών δεδομένων αποτελεί η συλλογή τους, με ειδοποιό σημείο το εάν συλλέγονται απευθείας από το υποκείμενο (άρθρο 13 ΓΚΠΔ), ή από άλλη πηγή (άρθρο 14 ΓΚΠΔ). Η πηγή συλλογής, καθώς και όλη η πορεία της επεξεργασίας επιβάλλεται να τίθενται διαφανώς εις γνώσιν των υποκειμένων, σύμφωνα με την αρχή της διαφάνειας, αποτυπωμένη στο άρθρο 13 ΓΚΠΔ.

Στο πραγματικό της συλλογής και επεξεργασίας δεδομένων για τη βιντεοεπιτήρηση του υποκειμένου, λόγω του ότι τα εν λόγω δεδομένα συλλέγονται μεν από το υποκείμενο, χωρίς ωστόσο κάποια δική του ενέργεια, έχουν διατυπωθεί δύο αντικρουόμενες απόψεις σχετικά με το ποιό εκ των άρθρων 13 και 14 ΓΚΠΔ εφαρμόζεται , με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), στις Κατευθυντήριες Γραμμές 3/2019 του, να συντάσσεται με το άρθρο 13, με την αιτιολογία πως η συλλογή δεδομένων από μια κάμερα αποτελεί συλλογή δεδομένων από το υποκείμενο, έστω και αν αυτό γίνεται χωρίς κάποια ενέργεια αυτού ή ακόμη και εν αγνοία του· στον αντί ποδα, στην απόφαση C-212/2013 (υπόθεση Rynes) το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) είχε παρεμ πιπτόντως αναφερθεί στην ενημέρωση του υποκειμέ νου για την επεξεργασία των δεδομένων του, όταν α υτά δε συλλέγονται απευθείας από αυτό, όπως επέτα σσε το τότε ισχύον (προ του ΓΚΠΔ) άρθρο 11 της Οδη γίας 46/1995, διάταξη που αντικατέστησε το άρθρο 14 του ΓΚΠΔ. Έκτοτε, το ΔΕΕ δεν έχει προβεί σε τοποθέτ ηση επί του θέματος, είτε πρωτογενώς, είτε υιοθετώντας ή αντικρούοντας, έστω, τις κατευθυντήριες του ΕΣΠΔ.

Σε αντίθεση με την πάγια θέση της πλειοψηφίας των Αρχών Προστασίας Προσωπικών Δεδομένων της ΕΕ, Η Σουηδική Δικαιοσύνη φαίνεται να διχάζεται ακόμα, αποστέλλοντας προδικαστικό ερώτημα στο ΔΕΕ, ζητώντας την ερμηνεία των άρθρων 13 και 14 του ΓΚΠΔ. Η υπόθεση ξεκίνησε όταν η Σουηδική Αρχή Προστασίας Δεδομένων επέβαλε Διοικητικό πρόστιμο ύψους 1.570.000 ευρώ (16 εκ. σουηδικές κορώνες), στην εταιρεία που διαχειρίζεται τις αστικές συγκοινωνίες της Στοκχόλμης, λόγω ελλειπούς ενημέρωσης των πολιτών για τις κάμερες που έφεραν στις στολές τους οι ελεγκτές. Η Αρχή στηρίχθηκε στην παραβίαση των υποχρεώσεων ενημέρωσης των υποκειμένων που προβλέπει το άρθρο 13 του ΓΚΠΔ. Η εταιρεία προσέφυγε στη Δικαιοσύνη, ζητώντας την ακύρωση του προστίμου και υποστηρίζοντας πως οι κάμερες δε συλλέγουν δεδομένα απευθείας από τα υποκείμενα και ως εκ τούτου δεν απαιτείται η ενημέρωσή τους, καθώς το άρθρο 14 του ΓΚΠΔ τυγχάνει εφαρμογής. Πράγματι, το πρόστιμο ακυρώθηκε εν μέρει, στο μέρος του που αφορούσε στην ελλειπή ενημέρωση. Η Σουηδική Αρχή προσέφυγε στο Ανώτατο Ακυρωτικό Δικαστήριο της χώρας, ζητώντας την αποστολή προδικαστικού ερωτήματος στο ΔΕΕ, για την οριστική επίλυση της διχογνωμίας. Πράγματι, εν αναμονή της εκδίκασης της υπόθεσης από το ΔΕΕ, το Σουηδικό Ανώτατο Ακυρωτικό παρατηρεί πως παρ'ότι το ΕΣΠΔ αποτελεί το καθύλην όργανο επιβολής της ομοιόμορφης επιβολής του ΓΚΠΔ, υπαρχόντων μάλιστα, επί του ζητήματος, των ανωτέρω αναφερθεισών Κατευθυντηρίων Γραμμών 3/2019, το ΔΕΕ δεν τις έχει επικαλεστεί ποτέ, αφήνοντας έδαφος για αμφιβολία.

Η χρήση (φορητών) συστημάτων επιτήρησης στην ελληνική έννομη τάξη

Σύμφωνα με το άρθρο 15 του ν. 3917/2011 που εξεδόθη κατόπιν των γνωμοδοτήσεων 1/2009 και 2/2010 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), ρυθμίζεται η χρήση συστημάτων επιτήρησης με λήψη ή και καταγραφή ήχου ή εικόνας σε δημόσιους χώρους, συνεπώς και των δημοσίων συγκοινωνιών.

Όπως ορίζεται στο άρθρο 14 του νόμου αυτού, η εγκατάσταση και λειτουργία τέτοιων συστημάτων επιτρέπεται για την αποτροπή και καταστολή εγκλημάτων κατά της δημόσιας τάξης, της ασφάλειας των συγκοινωνιών της ιδιοκτησίας, καθώς και κατά εγκλημάτων βίας και εμπορίας ναρκωτικών, όταν με βάση πραγματικά στοιχεία συντρέχουν επαρκείς ενδείξεις ότι τελέσθηκαν ή πρόκειται να τελεσθούν τέτοιες πράξεις. Μόνο κρατικές αρχές δύνανται να φέρουν τέτοια συστήματα, τηρουμένης της αρχής της αναλογικότητας και μόνο υπό τις προϋποθέσεις του Προεδρικού Διατάγματος 75/2020, το οποίο εξειδικεύει το νόμο.

Συγκεκριμένα για τις φορητές κάμερες επιτήρησης, αυτή επιτρέπεται σε περιπτώσεις που υπάρχει άμεσος σοβαρός κίνδυνος τέλεσης των ανωτέρω αναφερομένων εγκλημάτων, κατόπιν σχετικής αιτιολογημένης απόφασης του υπευθύνου επεξεργασίας δεδομένων, δηλαδή της εκάστοτε δημόσιας Αρχής.

Επιτρέπεται μόνο κατ' εξαίρεση η αποθήκευση και η διατήρηση των συλλεγέντων δεδομένων από την κάμερα, για διάστημα μεγαλύτερο των 15 ημερών, μόνο εάν υπάρχουν εύλογες υπόνοιες για τη διάπραξη, παρούσα ή επικείμενη, των ανωτέρω αδικημάτων.

Ομοίως, το ΔΕΕ έχει νομολογιακά[18] κηρύξει ανίσχυρη την Οδηγία 2006/24/ΕΚ (Data Retention Directive) για την υποχρεωτική διατήρηση των δεδομένων κίνησης και θέσης συνδρομητών και χρηστών από τους παρόχους τηλεπικοινωνιακών υπηρεσιών, προκειμένου να καθίστανται διαθέσιμα στις αρμόδιες αρχές για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων και αντιστοίχως, την Οδηγία 2002/58 ΕΚ (E- Privacy Directive), στη θέση της οποίας έχει ήδη κατατεθεί σχέδιο Κανονισμού E- Privacy, για τη διατήρηση τηλεπικοινωνιακών δεδομένων των συνδρομητών, για τον ίδιο ως άνω σκοπό της πρόληψης.

Θετική και αναμενόμενη κρίνουμε την περιοδική επανεξέταση και αναθεώρηση -ανά τακτά χρονικά διαστήματα- της αναγκαιότητας διατήρησης των δεδομένων, σύμφωνα με τις επιταγές των άρθρων 5 και 6 της Οδηγίας 680/2016, καθώς και 70 και 73 παρ. 4 του ν. 4624/2019.

---

[18] συνεκδικαζόμενες υποθέσεις Digital Rights Ireland Ltd C-293/12 και Kartner Landesregierung κ.λπ. C-594/12, απόφαση της 08-4-2014 ("Digital Rights Ireland") και συνεκδικαζόμενες υποθέσεις C-203/15 Tele2 Sverige AB και C-698/15 Secretary of State for the Home Department, απόφαση της 21-12-2016 ("Tele2").

Η Πράξη για την Τεχνητή Νοημοσύνη (AI Act)

Στις 12 Ιουλίου 2024 δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ο ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1689 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Ιουνίου 2024, ήτοι το τελικό κείμενο της προταθείσας ήδη από το 2021 Πράξης για την Τεχνητή Νοημοσύνη (Artificial Intelligence Act - στο εξής AI Act).

Στο παρόν θα γίνει σύντομη ανάλυση των καίριων σημείων της νέας ρύθμισης, που αποτελεί και την πρώτη παγκόσμια απόπειρα ορισμού και οριοθέτησης των συστημάτων τεχνητής νοημοσύνης, όσων δηλαδή επεξεργάζονται δεδομένα και παράγουν γνώση -ενίοτε και αποφάσεις-, που προσομοιάζουν με προϊόντα της ανθρώπινης διαννοίας. Πλέον, έχουμε περάσει στην εποχή της «παραγωγικής ή δημιουργικής ΤΝ».

Συνοπτική παρουσίαση της AI Act

Κατ'αρχάς, η AI Act ταξινομεί την ΤΝ ανάλογα με τον κίνδυνο που ενέχει:

Απαγορεύεται ο απαράδεκτος κίνδυνος (π.χ. συστήματα κοινωνικής βαθμολόγησης και η χειραγωγική ΤΝ).

Το μεγαλύτερο μέρος της ρύθμισης καταλαμβάνουν τα συστήματα ΤΝ υψηλού κινδύνου, ενώ, ένα μικρότερο τμήμα ασχολείται με τα συστήματα ΤΝ περιορισμένου κινδύνου, τα οποία υπόκεινται σε ελαφρύτερες υποχρεώσεις διαφάνειας: οι προγραμματιστές και οι φορείς ανάπτυξης πρέπει να διασφαλίζουν ότι οι τελικοί χρήστες γνωρίζουν ότι αλληλεπιδρούν με ΤΝ (chatbots και deepfakes).

Ο ελάχιστος κίνδυνος δεν ρυθμίζεται (συμπεριλαμβανομένης της πλειονότητας των εφαρμογών ΤΝ που είναι σήμερα διαθέσιμες στην ενιαία αγορά της ΕΕ, όπως τα βιντεοπαιχνίδια με χαρακτηριστικά ΤΝ.

Η πλειονότητα των υποχρεώσεων βαρύνει τους παρόχους (προγραμματιστές) συστημάτων ΤΝ υψηλού κινδύνου. Υποκείμενοι είναι οι πάροχοι εντός, αλλά και εκτός ΕΕ, όταν το συγκεκριμένο σύστημα παράγεται στην ΕΕ.

Οι χρήστες είναι φυσικά ή νομικά πρόσωπα που χρησιμοποιούν ένα σύστημα ΤΝ υπό επαγγελματική ιδιότητα, όχι οι επηρεαζόμενοι τελικοί χρήστες.

- Οι χρήστες (φορείς ανάπτυξης) των συστημάτων ΤΝ υψηλού κινδύνου έχουν ορισμένες υποχρεώσεις, αν και λιγότερες από τους παρόχους (προγραμματιστές).
- Αυτό ισχύει για τους χρήστες που βρίσκονται στην ΕΕ και για τους χρήστες τρίτων χωρών όταν η παραγωγή του συστήματος ΤΝ χρησιμοποιείται στην ΕΕ.

Τεχνητή νοημοσύνη γενικού σκοπού (General Purpose AI - GPAI):

Με τον όρο «μοντέλο ΤΝ γενικού σκοπού» νοείται το μοντέλο που είναι ικανό να εκτελεί με επάρκεια ένα ευρύ φάσμα διακριτών εργασιών, ανεξάρτητα από τον τρόπο διάθεσής του στην αγορά, και το οποίο μπορεί να ενσωματωθεί σε διάφορα συστήματα ή εφαρμογές.

Τα συστήματα αυτά μπορούν δυνητικά να χρησιμοποιηθούν ως συστήματα ΤΝ υψηλού κινδύνου ή να ενσωματωθούν σε αυτά. Οι πάροχοι συστημάτων ΓΓΠΙ θα πρέπει να συνεργάζονται με τέτοιους παρόχους συστημάτων ΤΝ υψηλού κινδύνου, ώστε να καταστεί δυνατή η συμμόρφωση των τελευταίων.

Όλοι οι πάροχοι μοντέλων Γενικού σκοπού πρέπει:

- Να συντάσσουν τεχνική τεκμηρίωση, συμπεριλαμβανομένης της διαδικασίας κατάρτισης και δοκιμών και των αποτελεσμάτων αξιολόγησης.
- Να συντάσσουν πληροφορίες και τεκμηρίωση για να παρέχουν στους μεταγενέστερους παρόχους που σκοπεύουν να ενσωματώσουν το μοντέλο ΓΓΠΙ στο δικό τους σύστημα ΤΝ, ώστε οι τελευταίοι να κατανοήσουν τις δυνατότητες και τους περιορισμούς και να μπορέσουν να συμμορφωθούν.
- Να καθιερώσουν πολιτική για τον σεβασμό της οδηγίας για τα πνευματικά δικαιώματα.
- Να δημοσιεύουν επαρκώς λεπτομερή περίληψη σχετικά με το περιεχόμενο που χρησιμοποιήθηκε για την εκπαίδευση του μοντέλου.

Τα δωρεάν και με ανοικτή άδεια χρήσης μοντέλα Γενικού σκοπού, - των οποίων οι παράμετροι, είναι δημόσια διαθέσιμες, επιτρέποντας την πρόσβαση, τη χρήση, την τροποποίηση και τη διανομή του μοντέλου - πρέπει να συμμορφώνονται μόνο με τις δύο τελευταίες παραπάνω υποχρεώσεις, εκτός εάν παρουσιάζονται συστημικοί κίνδυνοι.

Εκτός από τις τέσσερις παραπάνω υποχρεώσεις, οι πάροχοι μοντέλων Γενικού σκοπού με συστημικό κίνδυνο πρέπει επίσης:

- Να διενεργούν αξιολογήσεις υποδειγμάτων, συμπεριλαμβανομένης της διενέργειας και τεκμηρίωσης αντιφατικών δοκιμών για τον εντοπισμό και τον μετριασμό του συστημικού κινδύνου.
- Να αξιολογούν και να μετριάζουν πιθανούς συστημικούς κινδύνους, συμπεριλαμβανομένων των πηγών τους.
- Να παρακολουθούν, να τεκμηριώνουν και να αναφέρουν σοβαρά περιστατικά και πιθανά διορθωτικά μέτρα στο Ευρωπαϊκό Γραφείο ΤΝ και στις σχετικές εθνικές αρμόδιες αρχές χωρίς αδικαιολόγητη καθυστέρηση.
- Να διασφαλίζουν επαρκούς επιπέδου προστασία της ασφάλειας στον κυβερνοχώρο.
- Όλοι οι πάροχοι μοντέλων γενικού σκοπού που παρουσιάζουν συστημικό κίνδυνο -ανοικτής ή κλειστής άδειας- πρέπει επίσης να διενεργούν αξιολογήσεις μοντέλων, αντιπαραθετικές δοκιμές, να παρακολουθούν και να αναφέρουν σοβαρά περιστατικά και να διασφαλίζουν την προστασία της ασφάλειας στον κυβερνοχώρο.

Όλοι οι πάροχοι μοντέλων Γενικού σκοπού μπορούν να αποδείξουν τη συμμόρφωση με τις υποχρεώσεις τους εάν τηρούν εθελοντικά έναν κώδικα δεοντολογίας μέχρι να δημοσιευθούν ευρωπαϊκά εναρμονισμένα πρότυπα, η συμμόρφωση με τα οποία θα οδηγεί σε τεκμήριο συμμόρφωσης. Οι πάροχοι που δεν τηρούν κώδικες δεοντολογίας πρέπει να αποδείξουν εναλλακτικά επαρκή μέσα συμμόρφωσης για την έγκριση της Επιτροπής

Απαγορευμένα συστήματα τεχνητής νοημοσύνης (άρθρο 5 της AI Act)

Οι ακόλουθοι τύποι συστημάτων ΤΝ είναι "απαγορευμένοι" σύμφωνα με την AI Act.

- Όσα αναπτύσσουν υποσυνείδητες, χειριστικές ή παραπλανητικές τεχνικές για να στρεβλώσουν τη συμπεριφορά και να επηρεάσουν την τεκμηριωμένη λήψη αποφάσεων, προκαλώντας σημαντική βλάβη.
- Όσα εκμεταλλεύονται ευάλωτα ανθρώπινα χαρακτηριστικά όπως ηλικία, αναπηρία ή κοινωνικοοικονομικές συνθήκες για τη στρέβλωση της συμπεριφοράς τους, προκαλώντας σημαντική βλάβη.
- συστήματα βιομετρικής κατηγοριοποίησης που

συμπεραίνουν ευαίσθητα χαρακτηριστικά (φυλή, πολιτικά φρονήματα, συμμετοχή σε συνδικαλιστική οργάνωση, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, σεξουαλική ζωή ή σεξουαλικό προσανατολισμό), εκτός από την επισήμανση ή το φιλτράρισμα νομίμως αποκτηθέντων συνόλων βιομετρικών δεδομένων ή όταν η επιβολή του νόμου κατηγοριοποιεί βιομετρικά δεδομένα.

- Συστήματα κοινωνικής βαθμολόγησης, δηλαδή αξιολόγηση ή ταξινόμηση ατόμων ή ομάδων με βάση την κοινωνική συμπεριφορά ή τα προσωπικά χαρακτηριστικά, προκαλώντας δυσμενή μεταχείριση των ατόμων αυτών.
- Συστήματα αξιολόγησης του κινδύνου διάπραξης εγκληματικών πράξεων από ένα άτομο αποκλειστικά βάσει προφίλ ή χαρακτηριστικών της προσωπικότητας, εκτός εάν χρησιμοποιείται για την ενίσχυση των ανθρώπινων αξιολογήσεων που βασίζονται σε αντικειμενικά, επαληθεύσιμα γεγονότα που συνδέονται άμεσα με εγκληματική δραστηριότητα.
- Βάσεις δεδομένων αναγνώρισης προσώπου με μη στοχευμένη απόσπαση εικόνων προσώπου από το διαδίκτυο ή από υλικό από κάμερες κλειστού κυκλώματος παρακολούθησης.
- Συστήματα αναγνώρισης συναισθημάτων σε χώρους εργασίας ή εκπαίδευσης, εκτός αν συντρέχουν λόγοι υγείας ή ασφαλείας.
- Συστήματα που πραγματοποιούν εξ αποστάσεως βιομετρική ταυτοποίηση σε "πραγματικό χρόνο" σε δημόσια προσβάσιμους χώρους για την επιβολή του νόμου, εκτός εάν πρόκειται για:
    - αναζήτηση αγνοουμένων, θυμάτων απαγωγής και ατόμων που έχουν πέσει θύματα εμπορίας ανθρώπων ή σεξουαλικής εκμετάλλευσης,
    - αποτροπή ουσιαστικής και άμεσης απειλής για τη ζωή ή προβλέψιμης τρομοκρατικής επίθεσης- ή
    - εντοπισμό υπόπτων για σοβαρά εγκλήματα (π.χ. δολοφονίες, βιασμοί, ένοπλες ληστείες, διακίνηση ναρκωτικών και παράνομων όπλων, οργανωμένο έγκλημα και περιβαλλοντικό έγκλημα κ.λπ.)

Συστήματα ΤΝ υψηλού κινδύνου (Άρθρο 6 της AI Act)

Η νέα ρύθμιση ταξινομεί ορισμένα συστήματα ΤΝ ως "υψηλού κινδύνου". Οι πάροχοι αυτών των συστημάτων θα υπόκεινται σε πρόσθετες απαιτήσεις.

Κανόνες ταξινόμησης για συστήματα ΤΝ υψηλού κινδύνου (άρθρο 6)

Ως συστήματα ΤΝ υψηλού κινδύνου χαρακτηρίζονται όσα:

- χρησιμοποιούνται ως κατασκευαστικό στοιχείο ασφαλείας ή ως προϊόν που καλύπτεται από τη νομοθεσία της ΕΕ στο παράρτημα ΙΙ ΚΑΙ απαιτείται να υποβληθούν σε αξιολόγηση συμμόρφωσης από τρίτο μέρος σύμφωνα με την εν λόγω νομοθεσία του παραρτήματος ΙΙ- Ή
- Όσα εμπίπτουν στις περιπτώσεις χρήσης του παραρτήματος ΙΙΙ (κατωτέρω), εκτός εάν:
    - το σύστημα ΤΝ εκτελεί στενό διαδικαστικό έργο,
    - βελτιώνει το αποτέλεσμα μιας προηγουμένως ολοκληρωμένης ανθρώπινης δραστηριότητας,
    - ανιχνεύει πρότυπα λήψης αποφάσεων ή αποκλίσεις από προηγούμενα πρότυπα λήψης αποφάσεων και δεν προορίζεται να αντικαταστήσει ή να επηρεάσει την προηγουμένως ολοκληρωμένη ανθρώπινη αξιολόγηση

χωρίς κατάλληλη ανθρώπινη επανεξέταση- ή
    - εκτελεί προπαρασκευαστική εργασία για μια αξιολόγηση σχετική με τους σκοπούς των περιπτώσεων χρήσης που απαριθμούνται στο παράρτημα III.
- Τα συστήματα τεχνητής νοημοσύνης θεωρούνται πάντοτε υψηλού κινδύνου εάν δημιουργούν προφίλ ατόμων, δηλαδή αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων για την αξιολόγηση διαφόρων πτυχών της ζωής ενός ατόμου, όπως η εργασιακή απόδοση, η οικονομική κατάσταση, η υγεία, κ.α.

Απαιτήσεις για τους παρόχους συστημάτων ΤΝ υψηλού κινδύνου (άρθρα 8-25 της AIAct)

Οι πάροχοι συστημάτων ΤΝ υψηλού κινδύνου πρέπει:

- Να καθιερώσουν σύστημα διαχείρισης κινδύνου καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος ΤΝ υψηλού κινδύνου,
- Να διεξάγουν διακυβέρνηση δεδομένων, διασφαλίζοντας ότι τα σύνολα δεδομένων εκπαίδευσης, επικύρωσης και δοκιμών είναι συναφή, επαρκώς αντιπροσωπευτικά και, στον καλύτερο δυνατό βαθμό, απαλλαγμένα από σφάλματα και πλήρη σύμφωνα με τον επιδιωκόμενο σκοπό.
- Να συντάσσουν τεχνική τεκμηρίωση για την απόδειξη της συμμόρφωσης και να παρέχουν στις αρχές τις πληροφορίες για την αξιολόγηση της εν λόγω συμμόρφωσης.
- Να Σχεδιάζουν το σύστημα ΤΕ υψηλού κινδύνου για την τήρηση αρχείων, ώστε να μπορεί να καταγράφει αυτόματα γεγονότα σχετικά με τον εντοπισμό κινδύνων σε εθνικό επίπεδο και ουσιαστικών τροποποιήσεων καθ' όλη τη διάρκεια του κύκλου ζωής του συστήματος.
- Να παρέχουν οδηγίες χρήσης στους μεταγενέστερους φορείς ανάπτυξης, ώστε να καταστεί δυνατή η συμμόρφωση των τελευταίων.
- Να σχεδιάζουν το σύστημα ΤΝ υψηλού κινδύνου ώστε αυτό να είναι δεκτικό ανθρώπινης εποπτείας.
- Να Σχεδιάζουν το σύστημα ΤΝ υψηλού κινδύνου ώστε να επιτυγχάνουν τα κατάλληλα επίπεδα ακρίβειας, ευρωστίας και ασφάλειας στον κυβερνοχώρο.
- Να καθιερώσουν ένα σύστημα διαχείρισης ποιότητας που θα διασφαλίζει τη συμμόρφωση του συστήματος με την εθνική και Ενωσιακή νομοθεσία.

Στόχοι της νέας ρύθμισης

Για να αντληθούν τα μέγιστα δυνατά οφέλη από τα συστήματα ΤΝ, με παράλληλη προστασία των θεμελιωδών δικαιωμάτων, της υγείας και της ασφάλειας, οι πάροχοι, οι φορείς και τα θιγόμενα πρόσωπα θα πρέπει να εφοδιάζονται με τις απαραίτητες γνώσεις, ώστε να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τα συστήματα ΤΝ. Οι γνώσεις αυτές μπορούν να ποικίλλουν ανάλογα με το εκάστοτε πλαίσιο και μπορούν να περιλαμβάνουν κατανόηση της ορθής εφαρμογής των τεχνικών στοιχείων κατά τη φάση ανάπτυξης του συστήματος ΤΝ, τα μέτρα που πρέπει να εφαρμόζονται κατά τη χρήση του, τους κατάλληλους τρόπους ερμηνείας των στοιχείων εξόδου του συστήματος ΤΝ, καθώς και, στην περίπτωση των θιγόμενων προσώπων, τις γνώσεις που απαιτούνται για να κατανοούν πώς θα τα επηρεάσουν οι αποφάσεις που λαμβάνονται με τη βοήθεια της ΤΝ.

Σύμφωνα με δελτίο τύπου του Ελληνικού Υπουργείου Εσωτερικών, τον προσεχή Σεπτέμβριο εκκινούν εκπαιδευτικά προγράμματα για τους δημοσίους

υπαλλήλους, αναφορικά με τη χρήση συστημάτων ΤΝ. Οι πρώτοι 500 υπάλληλοι έχουν αρχίσει πιλοτικά την εκπαίδευση.

Προκειμένου να διασφαλιστούν ισότιμοι όροι ανταγωνισμού και αποτελεσματική προστασία των δικαιωμάτων και των ελευθεριών των ατόμων σε ολόκληρη την Ένωση, οι κανόνες που θεσπίζονται με την AI Act έχουν εξωεδαφική εφαρμογή, ήτοι ισχύουν ομοιόμορφα για παρόχους συστημάτων ΤΝ είτε είναι εγκατεστημένοι στην ΕΕ, είτε σε Τρίτη χώρα.

Χρονοδιάγραμμα εφαρμογής

Από την ψήφησή της, 13 Ιουνίου 2024, η AI Act θα ακολουθήσει σταδιακή εφαρμογή, με ημερομηνία επίσημης θέσης σε ισχύ την 1η Αυγούστου 2024 και πλήρους εφαρμογής την 2η Αυγούστου 2026,ότελήγει και η προθεσμία των κρατών-μελών να ορίσουν τις εθνικές αρμόδιες αρχές, οι οποίες θα εποπτεύουν την εφαρμογή των κανόνων για τα συστήματα ΤΝ, καθώς και τη σχετική αγορά:

- 6 μήνες για τα απαγορευμένα συστήματα ΤΝ.
- 12 μήνες για τα συστήματα ΤΝ γενικού σκοπού
- 24-36 μήνες για συστήματα ΤΝ υψηλού κινδύνου
- 9 μήνες για τους κώδικες δεοντολογίας

Προκειμένου να καλυφθεί η μεταβατική περίοδος πριν από την πλήρη εφαρμογή του κανονισμού, η Επιτροπή δρομολόγησε το σύμφωνο για την ΤΝ. Η εν λόγω πρωτοβουλία καλεί τους προγραμματιστές ΤΝ να υιοθετήσουν οικειοθελώς τις βασικές υποχρεώσεις της AI Act πριν από τις νόμιμες προθεσμίες.

Η Υπηρεσία ΤΝ της Επιτροπής θα είναι ο κύριος φορέας εφαρμογής του κανονισμού για την ΤΝ σε επίπεδο ΕΕ, καθώς και ο εγγυητής των κανόνων για τα μοντέλα ΤΝ γενικού σκοπού.

Η ρύθμιση της Τεχνητής Νοημοσύνης πέρα από τον Ατλαντικό

Λαμβάνοντας υπόψη το γεγονός ότι οι πρωτοπόροι στην ανάπτυξη συστημάτων τεχνητής νοημοσύνης βρίσκονται εκτός της ΕΕ και, κυρίως την παρούσα τουλάχιστον περίοδο, στις ΗΠΑ είναι χρήσιμο να εξετάσουμε πώς αντιμετωπίζεται νομικά η ρύθμιση της ανάπτυξης των συστημάτων τεχνητής νοημοσύνης στις ΗΠΑ. Η εξωεδαφική εφαρμογή της πράξης για την τεχνητή νοημοσύνη δύναται να έχει σημαντικές επιπτώσεις για τις εταιρείες και τους υπεύθυνους χάραξης πολιτικής στις ΗΠΑ καθώς γεωγραφική εμβέλεια τη πράξης σημαίνει ότι οι αμερικανικές εταιρείες πρέπει να συμμορφώνονται με τις υποχρεώσεις που προβλέπει εάν τα συστήματα τεχνητής νοημοσύνης τους χρησιμοποιηθούν από πελάτες της ΕΕ προσαρμόζοντάς πρακτικές ανάπτυξης και διακυβέρνησης της τεχνητής νοημοσύνης.

Από πλευράς νομοθετικών ρυθμίσεων και πρωτοβουλιών επί του παρόντος, είτε έχουν ψηφιστεί είτε εκκρεμούν σε επίπεδο επιμέρους πολιτειών πολυάριθμα νομοθετήματα[19]. Η πλέον σημαντική πρωτοβουλία σε εθνικό (ομοσπονδιακό) επίπεδο είναι το εκτελεστικό διάταγμα (ΕΔ) για την τεχνητή νοημοσύνη που εξέδωσε ο Πρόεδρος Μπάιντεν στις 30 Οκτωβρίου 2023, με στόχο την ασφαλή, προστατευμένη και αξιόπιστη ανάπτυξη και χρήση της τεχνητής νοημοσύνης[20].

Είναι προφανές ότι τόσο η ΕΕ όσο και οι Ηνωμένες Πολιτείες αναγνωρίζουν τις δυνατότητες της τεχνητής νοημοσύνης και τη σημασία της διαχείρισης των κινδύνων της. Αυτή η κοινή αντίληψη οδήγησε στην υιοθέτηση μιας κινδυνοκεντρικής προσέγγισης, δίνοντας έμφαση στην ανάγκη ελέγχου και ρύθμισης των εφαρμογών τεχνητής νοημοσύνης που θεωρούνται. Και τα δύο νομοθετήματα αναγνωρίζουν την αναγκαιότητα:

- Διεξαγωγής αυστηρών δοκιμών και παρακολούθησης - δίνεται έμφαση στη συνεχή αξιολόγηση των συστημάτων ΤΝ, ώστε να διασφαλίζεται ότι είναι ασφαλή, αξιόπιστα και λειτουργούν όπως προβλέπεται, από τις δοκιμές πριν από την ανάπτυξη έως την εποπτεία μετά τη διάθεση στην αγορά.
- Προστασίας δεδομένων. Τονίζεται η σημασία της προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής των ατόμων κατά την ανάπτυξη και την εγκατάσταση συστημάτων τεχνητής νοημοσύνης.
- Ασφάλειας στον κυβερνοχώρο. Δίνεται βαρύτητα στην ανάγκη για ισχυρά μέτρα ασφάλειας στον κυβερνοχώρο, υποστηρίζοντας την «ασφάλεια από το σχεδιασμό» για την προστασία από κακή χρήση και εξωτερικές απειλές.

Σύγκριση των ρυθμιστικών μοντέλων ΕΕ & ΗΠΑ

Εντούτοις, η σύγκλιση σταματά στις θεμελιώδεις αρχές και στόχους καθώς η μέθοδος επίτευξης των κοινών σκοπών είναι διαφορετική.

Από την πλευρά της, η ΕΕ επέλεξε την υιοθέτηση μιας άμεσα εφαρμόσιμης ολοκληρωμένης νομικής δομής, η οποία καθορίζει σαφώς τις υποχρεώσεις, τις απαγορεύσεις και τους μηχανισμούς επιβολής για τα

[19] Βλ. United States approach to artificial intelligence, διαθέσιμο στο https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pd

[20] Βλ. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

συστήματα ΤΝ με βάση το επίπεδο κινδύνου τους. Από την Στον αντίποδα, οι ΗΠΑ υιοθέτησαν μια προσέγγιση βασισμένη σε αρχές, ενθαρρύνοντας την υπεύθυνη ανάπτυξη ΤΝ μέσω γενικών κατευθυντηρίων γραμμών που δίνουν έμφαση στην ασφάλεια, την καινοτομία και τη δεοντολογία. Ακολουθείται η πάγια λογική της αυτορρύθμισης και της παροχής ευχέρειας στις πολιτείες να θεσπίζουν νομοθεσία. Ως εκ τούτου, ελλείψει δεσμευτικού ομοσπονδιακού νόμου, αναμένεται κάποιες πολιτείες να αναλάβουν τα ηνία στην εισαγωγή κανονιστικού πλαισίου για την τεχνητή νοημοσύνη.

Η ΕΕ θεσπίζει ένα αυστηρό καθεστώς εφαρμογής της πράξης για την τεχνητή νοημοσύνη, με δυνατότητα επιβολής σημαντικών προστίμων, σηματοδοτώντας μια ισχυρή δέσμευση για συμμόρφωση. Αντίθετα, η προσέγγιση των ΗΠΑ, στερείται συγκεκριμένων κυρώσεων για μη συμμόρφωση και βασίζεται περισσότερο στην εθελούσια εφαρμογή των κατευθυντηρίων γραμμών και στην αυτορρύθμιση των εμπλεκομένων μερών του κλάδου.

Τέλος, η πράξη της ΕΕ για την τεχνητή νοημοσύνη αποσκοπεί στην ομοιομορφία, επιδιώκοντας να εφαρμόσει ένα ενιαίο κανονιστικό πλαίσιο σε όλα τα κράτη μέλη, μειώνοντας έτσι τον κατακερματισμό του κανονιστικού πλαισίου. Η στρατηγική των ΗΠΑ, επιτρέποντας στις επί μέρους πολιτείες να υιοθετήσει κάθε μία ξεχωριστή ρύθμιση μπορεί να οδηγήσει σε διαφορετικές ερμηνείες και εφαρμογές εντός της επικράτειας.

Θα γεφυρωθεί τελικά η απόσταση;

Οι διαφορές μεταξύ των προσεγγίσεων της ΕΕ και των ΗΠΑ όσον αφορά τη ρύθμιση της τεχνητής νοημοσύνης αντικατοπτρίζουν ουσιαστικές φιλοσοφικές και πρακτικές διαφορές στη διακυβέρνηση, τη νομική παράδοση και τη στάση απέναντι στη ρύθμιση της αγοράς και στη ραγδαία τεχνολογική εξέλιξη. Το «μπαράζ» των αντιδράσεων έχουν ήδη ξεκινήσει: Ήδη η Meta δήλωσε ότι δεν θα εισάγει τα μοντέλα Meta AI στην ΕΕ, τουλάχιστον επί του παρόντος, από την στιγμή που η Ιρλανδική Εποπτική Αρχή ζήτησε την καθυστέρηση του σχεδίου της να αξιοποιήσει δεδομένα από χρήστες του Facebook και του Instagram, για σκοπούς εκπαίδευσης των μοντέλων τεχνητής νοημοσύνης χωρίς την λήψη συγκατάθεσης των υποκειμένων (κατόπιν προσφυγών από το NOYB στις αρχές προστασίας δεδομένων στην Αυστρία, το Βέλγιο, τη Γαλλία, τη Γερμανία, την Ελλάδα, την Ιταλία, την Ιρλανδία, τις Κάτω Χώρες, τη Νορβηγία, την Πολωνία και την Ισπανία εναντίον της Meta). Ομοίως τον Ιούνιο του 2024 η Apple δήλωσε ότι δεν θα κυκλοφορήσει τις λειτουργίες της Apple Intelligence στην Ευρώπη λόγω « προβληματισμών επί του κανονιστικού πλαισίου» αναφερόμενη στο Digital Markets Act[21].

Σε επίπεδο ρυθμιστικών αρχών, ωστόσο, παρουσιάζεται μία διάθεση συνεργασίας και σύμπραξης όπως προκύπτει από το κοινό ανακοινωθέν της ομοσπονδιακής επιτροπής εμπορίου (FTC), του Υπουργείου Δικαιοσύνης των ΗΠΑ, της Αρχής Ανταγωνισμού και Αγορών του Ηνωμένου Βασιλείου και της Margrethe Vestager, εκτελεστική αντιπρόεδρος και επίτροπος ανταγωνισμού για την Ευρωπαϊκή Επιτροπή, επιβεβαιώνοντας τη δέσμευσή για την προστασία του ανταγωνισμού σε όλο το οικοσύστημα τεχνητής νοημοσύνης (AI) για τη διασφάλιση αποτελεσματικού ανταγωνισμού που παρέχει δίκαιη και ειλικρινή

[21] Βλ. Apple says it won't roll out AI features in Europe due to regulatory concerns https://www.axios.com/2024/06/21/apple-ai-features-europe

μεταχείριση τόσο για τους καταναλωτές όσο και για τις επιχειρήσεις.

Καθίσταται φανερό ότι παρά τις ουσιώδεις διαφορές, η εξέλιξη των τεχνολογιών τεχνητής νοημοσύνης, ο συνεχιζόμενος διάλογος μεταξύ των παγκόσμιων δυνάμεων είναι ζωτικής σημασίας για τη διαμόρφωση ενός συνεκτικού, υπεύθυνου ρυθμιστικού πλαισίου που μπορεί να προσαρμοστεί στις αναδυόμενες προκλήσεις και ευκαιρίες. Οι εταιρείες θα πρέπει να παραμείνουν ευέλικτες και καλά ενημερωμένες σε αυτό το εξελισσόμενο κανονιστικό τοπίο, όχι μόνο για λόγους συμμόρφωσης, αλλά και ως στρατηγική επιταγή για καινοτομία και ηγετική θέση σε ένα υπεύθυνο οικοσύστημα τεχνητής νοημοσύνης.

ΑΥΓΟΥΣΤΟΣ 2024

TMT & PRIVACY

Ομάδα TMT & Privacy

Σπύρος Τάσσης, Partner, spiros.tassis@potamitisvekris.com

Παναγιώτα Κέλαλη, Senior Associate, panagiota.kelali@potamitisvekris.com

Αιμίλιος-Αρτέμιος Στραγαλινός, Associate, aimilios.stragalinos@potamitisvekris.com

Δήμητρα Ιορδανίδου, Associate, dimitra.iordanidou@potamitisvekris.com

Σοφία Τσιπουρίδη-Παρασκευοπούλου, Associate sofia.tsipouridi@potamitisvekris.com

Ελένη Βλιώρα, Associate eleni.vliora@potamitisvekris.com

Άννα Φαφαλιού, Trainee anna.fafaliou@potamitisvekris.com

Αγγελική Ζαφειροπούλου, Trainee angeliki.zafiropoulou@potamitisvekris.com