BLOCKCHAIN ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ: ΡΗΓΜΑΤΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΚΗ ΟΥΔΕΤΕΡΟΤΗΤΑ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ ΕΚ 679/2016 (ΓΚΠΔ)

Ελένη Κατωπόδη
Δικηγόρος Αθηνών,
Επιστημονική Συνεργάτης στο Τεχνικό Πανεπιστήμιο του Μονάχου και υποψήφια Διδάκτορας του Πανεπιστημίου του Augsburg

ΠΕΡΙΛΗΨΗ

Η τεχνολογία blockchain έδωσε την αφορμή έγερσης πολλών κανονιστικών ερωτημάτων, συμπεριλαμβανομένων και ερωτημάτων που σχετίζονται με την εφαρμογή του Κανονισμού ΕΚ 679/2016 (ΓΚΠΔ) για τα προσωπικά δεδομένα, στις περιπτώσεις επιχειρήσεων που λειτουργούν σε αποκεντρωμένη βάση. Παρά το γεγονός ότι ο Κανονισμός εξοπλίζεται με εγγυήσεις τεχνολογικής ουδετερότητας από τα Ενωσιακά όργανα, κάποια εγγενή γνωρίσματα των blockchains φαίνεται να έρχονται σε σύγκρουση με την ισχύουσα ρύθμιση και θεωρητική προσέγγιση του ΓΚΠΔ.

ABSTRACT

Blockchain technology has given rise to many regulatory questions, including questions related to the application of Regulation 679/2016 (GDPR) on personal data in the case of companies operating on a decentralized basis. Even though the Regulation is equipped with technological neutrality guarantees by the EU institutions, some inherent features of blockchains seem to create tension with the current regulation and theoretical approach of the GDPR.

I. ΕΙΣΑΓΩΓΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Κατά την προσπάθεια ρύθμισης του διαδικτύου, ο καθηγητής Lawrence Lessig[1] του Πανεπιστημίου του Harvard ανέπτυξε μια θεωρία, γνωστή ως η «pathetic dot theory», η οποία περιέγραφε πώς η ανθρώπινη συμπεριφορά μπορεί να ελεγχθεί από τέσσερις εξωτερικούς παράγοντες: Τον νόμο, τις κοινωνικές

[1] L. Lessig, *Code: version 2.0*, 2006, σελ. 123-124.

νόρμες, τον νόμο της αγοράς που θεμελιώνεται με άξονες την προσφορά και τη ζήτηση και την αρχιτεκτονική που διέπει τον υλικό και τον ψηφιακό κόσμο[2]. Γίνεται αντιληπτό ότι ο πλέον διαδεδομένος και άμεσος τρόπος επιβολής υποχρεώσεων και απαγορεύσεων στο πρόσωπο είναι η κανονιστική ρύθμιση. Στην περίπτωση αυτή, το πρόσωπο είτε θα συμμορφωθεί και θα απόσχει από τις απαγορευμένες συμπεριφορές ή θα υποστεί την κύρωση με οποιαδήποτε μορφή. Ο νόμος λοιπόν δρα με παιδευτική και διαμορφωτική λειτουργία και εν πολλοίς θέτει όρια στη χρήση των νέων καινοτομιών.

Ενόψει της παρούσας μελέτης, η προβληματική ελλοχεύει κανονιστικά σε σχέση με την εφαρμογή της προϋπάρχουσας ρύθμισης στην τεχνολογία blockchain. Η τεχνολογία κατανεμημένου καθολικού, ευρύτερα γνωστή ως τεχνολογία blockchain, το πρώτον εμφανίστηκε μέσα από τον τομέα των κρυπτονομισμάτων, όπως το Bitcoin και το Ethereum, σύντομα ωστόσο διαφοροποιήθηκε και αναδείχτηκαν οι ευρύτερες χρήσεις της σε πολλούς τομείς της οικονομίας. Το blockchain συνεχίζει τις εξελίξεις και τις προβληματικές που ξεκίνησαν με τη θεμελίωση του *World Wide Web* λίγες δεκαετίες προηγουμένως.

Από την άλλη, το δικαίωμα στον ιδιωτικό βίο και η αρνητική έκφανσή του ως το δικαίωμα στη διαγραφή ή τη λήθη έχουν εμπνεύσει πλούσια νομοθετική παραγωγή και έχουν τύχει ευρέος διαλόγου, κυρίως σε ενωσιακό επίπεδο. Στην πραγματικότητα, το δικαίωμα στην ιδιωτική σφαίρα με την έννοια της προστασίας των προσωπικών δεδομένων εξοπλίζεται με συνταγματική περιωπή από το εν έτει 2001 εισαχθέν άρθρο 9^{A} του ελληνικού Συντάγματος[3], ενώ σε ενωσιακό επίπεδο τυγχάνει εφαρμογής ο Γενικός Κανονισμός ΕΚ 679/2016 για την προστασία Δεδομένων Προσωπικού Χαρακτήρα[4] (στο εξής: ΓΚΠΔ), ερειδόμενος στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Δυστυχώς, παρά την πρόθεση του Ενωσιακού νομοθέτη να εξοπλίσει τον νέο τότε Κανονισμό με εγγυήσεις τεχνολογικής ουδετερότητας[5], ώστε να καταλογιστούν ευθύνες σε επιχειρήσεις ανεξαρτήτως του λειτουργικού συστήματος ή του τρόπου οργάνωσης που χρησιμοποιούν, μέχρι σήμερα ερείδεται και λειτουργεί αποτελεσματικά επί τη βάση μη-αποκεντρωμένων συστημάτων[6]. Τα μη-αποκεντρωμένα συστήματα συνιστούν δομές που ανταποκρίνονται σε ένα κάθετο-ιεραρχικό επίπεδο με ορισμένα νομικά ή φυσικά πρόσωπα ως φορείς, και κατ' επέκτασιν ως ενεχόμενους σε περιπτώσεις καταλογισμού ευθύνης. Αντιθέτως, η τεχνολογία κατανεμημένου καθολικού[7] (DLT), στη βασικότερη έκφανσή της, το blockchain, κατάφερε να προκαλέσει μια μεταβολή στον τρόπο που αντιλαμβάνεται ο μέσος χρήστης την αποθήκευση δεδομένων, καθώς βασίζεται ως επί το πλείστον σε μια αποκεντρωμένη συλλογή δεδομένων. Στο πλαίσιο αυτό, ο κάθε χρήστης ως συμμετέχων στο

---

[2] P. De Filippi/A. Wright, *Blockchain and the Law*, 2018, σελ. 173.

[3] Βλ. για τη συνταγματική ερμηνεία και ανάλυση των άρθρων 9 και 9^{A}, Κ. Χρυσόγονο, *Ατομικά και Κοινωνικά Δικαιώματα*, 3η έκδοση, 2006, σελ. 250-256, Β. Χρήστου, *Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων*, 2017 και Κ. Γ Μαυριά, *Το Συνταγματικό Δικαίωμα Ιδιωτικού Βίου*, 1982, σελ. 158-159.

[4] ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

[5] Λ. Μήτρου, *Ο γενικός κανονισμός προστασίας δεδομένων*, 2017, σελ. 54.

[6] M. Artzt/L. Determann/W. Long, «Chapter 5: Blockchain and Data Privacy», σε M. Artzt/T. Richter (επιμ.), *Handbook of Blockchain Law*, 2020, σελ. 200.

[7] Ελληνική απόδοση του αγγλικού όρου «distributed ledger technology».

σύστημα επεξεργάζεται και αποθηκεύει στον υπολογιστή του ένα αντίγραφο των δεδομένων του συστήματος, λειτουργώντας έτσι ως «αποκεντρωμένος server» στο γενικό δίκτυο[8]. Με αυτό τον τρόπο, επιτυγχάνεται η θεμελίωση πίστης στο σύστημα και η αποφυγή ενδιάμεσων μεσολαβητών. Η αντίρροπη τελεολογία του Κανονισμού και της τεχνολογίας εγείρει δικαιολογημένη ανησυχία στο ενδεχόμενο που η κανονιστική ρύθμιση περιστείλει για άλλη μια φορά την καινοτομία που αναμένεται να εδραιωθεί. Από την άλλη, η δύσκαμπτη διατύπωση και οπτική του Κανονισμού ενδέχεται να ευνοήσει επιχειρήσεις διαφορετικής οργάνωσης που αρύονται τα τεχνολογικά τους προνόμια για να υποσκάψουν την ισχύ του νόμου.

Η παρούσα μελέτη στοχεύει να διαφωτίσει ειδικότερες εκφάνσεις του προβλήματος, αναδεικνύοντας τα μείζονα πρακτικά προβλήματα κατά την ερμηνεία και την εφαρμογή του ΓΚΠΔ. Το πρώτον, εκπονείται μια θεωρητική προσέγγιση στη στοχοθεσία και τον τρόπο λειτουργίας της τεχνολογίας blockchain, με έμφαση στα πιο κρίσιμα χαρακτηριστικά της. Δεύτερον, καταδεικνύονται τα βασικότερα σημεία που πρέπει να συγκεντρωθεί το ερμηνευτικό βάρος κατά την εφαρμογή του ΓΚΠΔ σε αποκεντρωμένα συστήματα. Τρίτον, εκπονείται μνεία στην εννοιολογική επισκόπηση του δικαιώματος στη λήθη και, καταληκτικά, η ερμηνεία της αρχής της αναλογικότητας στο πλαίσιο της προστασίας προσωπικών δεδομένων μέσω ψηφιακών συστημάτων τύπου blockchain.

II. Η ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN

1. Λειτουργία και τεχνικά γνωρίσματα της τεχνολογίας blockchain

Η τεχνολογία κατανεμημένου καθολικού (*DLT*) συνιστά μια βασική υποδομή για την καταγραφή και αποθήκευση στοιχείων σε αποκεντρωμένη βάση, δηλαδή σε αποκεντρωμένο δίκτυο πολλών υπολογιστών[9]. Τον πιο συνήθη τύπο DLT συνιστά η τεχνολογία blockchain, με τους δύο όρους να χρησιμοποιούνται πλέον σχεδόν ταυτόσημα στην πράξη. Ιστορικά, η ανάπτυξη της καινοτομίας αυτής μπορεί να υποληφθεί ως μια άμεση τεχνολογική αντανακλαστική αντίδραση στην συγκέντρωση όγκων δεδομένων σε κεντρικές βάσεις και, άμα τη εισαγωγή της στην αγορά, συνδέθηκε στενά με τον τομέα των επενδύσεων και τα κρυπτονομίσματα, όπως το Bitcoin ή το Ethereum, εν είδει σύγχρονων μορφών νομίσματος στις συναλλαγές. Ωστόσο, στην πράξη αποδείχτηκε ότι το χρηματοπιστωτικό σύστημα συνιστά μόνο έναν βασικό τομέα, στον οποίο η τεχνολογία μπορεί να εφαρμοστεί.

Τα λειτουργικά συστήματα blockchain κρυπτογραφούν την ταυτότητα των χρηστών, επιτρέποντας παράλληλα την ψηφιακή ταυτοποίησή τους από το σύστημα μέσω της διαδικασίας αυθεντικοποίησης των δύο προσωπικών κλειδιών. Τα κλειδιά αυτά συνιστούν την ψηφιακή υπογραφή του χρήστη. Το δημόσιο κλειδί είναι το εμφανές αναγνωριστικό γνώρισμα του χρήστη και είναι αυτό που μοιράζεται με τα υπόλοιπα μέλη του συστήματος όταν συναλλάσσεται[10]. Το ιδιωτικό κλειδί πρέπει να φυλάσσεται σε ασφαλές μέρος από τον χρήστη και δεν είναι κοινοποιήσιμο. Έτσι, κάθε φορά που εκτελείται μια συναλλαγή απελευθερώνεται στον αποκεντρωμένο ιστό χρηστών, οι οποίοι οφείλουν να επιβεβαιώσουν/επαληθεύσουν τη συναλλαγή, προκειμένου αυτή να προστεθεί

[8] N. Marnau, «Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung», σε M. Eibl/ M. Gaedke, *INFORMATIK 2017*, link, σελ. 1025-1026, (τελευταία πρόσβαση 31.07.2022).
[9] Link, (τελευταία πρόσβαση 01.08.2022).
[10] Link, (τελευταία πρόσβαση 31.07.2022).

στην αλυσίδα και να χρησιμοποιηθεί για την παραγωγή της επόμενης δεσμίδας (*block*). Με αυτό τον τρόπο, η ταυτότητα του χρήστη παραμένει πάντοτε ανώνυμη, χωρίς ταυτόχρονα να εγείρονται αμφιβολίες σχετικά με την αξιοπιστία του ή να επαφίεται η επαλήθευση σε έναν κεντρικό μεσολαβητή. Μετά την έγκρισή της από το σύστημα, η συναλλαγή και τα δεδομένα που αυτή περιέχει απελευθερώνονται στην αλυσίδα και αποθηκεύονται στον αποκεντρωμένο ιστό με μη αναστρέψιμο τρόπο. Τούτο συνεπάγεται ότι σε περίπτωση λάθους, μήτε οι χρήστες μήτε οι προγραμματιστές διαθέτουν τη δυνατότητα υποβολής διορθώσεων ή διαγραφής. Η ιδιότητα αυτή των blockchain συστημάτων καθίσταται αναγκαία προκειμένου να επιλυθεί το υπολογιστικό πρόβλημα του *double spending*[11] που είναι ιδιαιτέρως δημοφιλές με τα ψηφιακά χρήματα.

Το βασικότερο, όμως, που κατάφερε να πετύχει η τεχνολογία blockchain είναι η μετατόπιση της εμπιστοσύνης των χρηστών από τον ανθρώπινο παράγοντα (τράπεζες, μεσίτες, λοιπούς χρηματοπιστωτικούς φορείς) σε ένα απρόσωπο, απέραντο σύστημα, το οποίο λειτουργεί επί τη βάση ορισμένων, *a priori* γνωστών κανόνων[12]. Οι κανόνες αυτοί λειτουργούν εν είδει μιας εσωτερικής οργανωτικής τάξης για το blockchain από όλους τους χρήστες απαρέγκλιτα και είναι ο λόγος αποφυγής μιας κεντρικής δομής εξουσίας, ο λόγος επίτευξης αποκεντρωμένου συντονισμού (αποκέντρωση και αποδιαμεσολάβηση). Από αυτά τα δύο χαρακτηριστικά προκύπτουν ωστόσο όλα τα σημαντικότερα πλεονεκτήματα της τεχνολογίας blockchain για τους χρήστες των συστημάτων, αντίστοιχα η μεγιστοποίηση της ασφάλειας των δεδομένων, η απλούστευση της επεξεργασίας των συμβάσεων και η μείωση του κόστους των συναλλαγών.

2. Κατηγοριοποίηση συστημάτων blockchain

Τα υπάρχοντα συστήματα που βασίζονται στην τεχνολογία blockchain δύνανται να κατηγοριοποιηθούν ενόψει των ιδίων γνωρισμάτων τους σε συστήματα δημόσια ή ιδιωτικά[13], περιορισμένης ή ελεύθερης πρόσβασης[14]. Το 2019 το Ευρωπαϊκό Κοινοβούλιο εξέδωσε μελέτη αναφορικά με τη συνύπαρξη των κανόνων για τα προσωπικά δεδομένα, ιδίως του ισχύοντος Γενικού Κανονισμού, σε συστήματα blockchain[15]. Σε αυτήν αναγνωρίζεται η ανάγκη περαιτέρω ερμηνείας και επιστημονικής έρευνας, καθώς η τεχνολογία blockchain αφενός δεν εκτείνεται σε αποκεντρωμένη βάση, αφετέρου δεν περιλαμβάνει σε κάθε περίπτωση υποκείμενα επεξεργασίας και επιχειρήσεις εντός της ΕΕ. Ως προς το γεγονός αν ο ΓΚΠΔ θεωρητικά εφαρμόζεται ή έστω δύναται να εφαρμοστεί ως προς τα γεωγραφικά του όρια και στα συστήματα τεχνολογίας κατανεμημένου καθολικού, δεν καταλείπεται αμφιβολία. Η ευρεία διατύπωση του άρθρου 3 αρκεί για να καλύψει τα ερμηνευτικά

[11] Το φαινόμενο του double spending είναι εμφανές όταν ένα ψηφιακό νόμισμα διπλασιάζεται στο σύστημα και μπορεί να ξοδευτεί παραπάνω από μία φορές από τον χρήστη. Για εκτενέστερη ανάλυση, βλ. J. Kroll/I. Davey/E. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, The Twelfth Workshop on the Economics of Information Security* (WEIS 2013), 11-12.06.2013, link, σελ. 1, (τελευταία πρόσβαση 11.08.2022).

[12] Baur/Brügmann/Sedlmeir/Urbach, «I. Grundlegende Eigenschaften der Blockchain-Technologie, §8», σε A. Leopold/A. Wiebe/S. Glossner, *Münchener Anwaltshandbuch IT-Recht*, 2021.

[13] Η διάκριση μεταξύ δημοσίων/ανοιχτών (*public*) και ιδιωτικών/κλειστών (*private*) blockchains σχετίζεται με το πόσοι ή ποιοι είναι σε θέση να έχουν πρόσβαση (παθητικά) στα δεδομένα του συστήματος (*reading rights*).

[14] Η διάκριση μεταξύ περιορισμένης (*permissioned*) και ελεύθερης (*permissionless*) πρόσβασης blockchain σχετίζεται με το πόσοι ή ποιοι είναι σε θέση να επέμβουν ενεργητικά στο σύστημα και να προκαλέσουν αλλαγές (*writing rights*)

[15] EPRS | European Parliamentary Research Service, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?,* link, σελ. 37, (τελευταία πρόσβαση 11.08.2022).

κενά· συνεπαγομένου στην περίπτωση των ιδιωτικών και περιορισμένων blockchain, ο τελευταίος θα εφαρμόζεται σε κάθε νομικό πρόσωπο που διαχειρίζεται το λειτουργικό. Η προβληματική συσχέτιση των συστημάτων με τα προσωπικά δεδομένα κυρίως σχετίζεται με τα δημόσια συστήματα ελεύθερης πρόσβασης, καθώς τα κλειστά, περιορισμένης πρόσβασης συστήματα προσιδιάζουν στις συμβατικές εταιρικές δομές, εφόσον δεν είναι δημόσια και οι χρήστες χρειάζονται άδεια ή έγκριση του VPN τους προκειμένου να εισέλθουν στο σύστημα, και έτσι δεν εγείρουν ιδιαίτερες αμφιβολίες σε ζητήματα εφαρμογής του ΓΚΠΔ. Ως προς αυτά ισχύουν οι γενικές προϋποθέσεις του ΓΚΠΔ ως προς την προστασία της επεξεργασίας δεδομένων, και η τεχνολογική ουδετερότητα και η δομή του Κανονισμού επιτρέπουν την αναλογική εφαρμογή των διατάξεων μέσω ερμηνείας. Η δεύτερη κατηγορία blockchain συστημάτων, τα δημόσια συστήματα, και ιδίως αυτά που επιτρέπουν την ελεύθερη πρόσβαση σε κάθε χρήστη, ενδείκνυται για περαιτέρω επιστημονική διερεύνηση. Ως προς αυτά, ο Κανονισμός θα αφορά κάθε συμμετέχοντα στην ΕΕ, ο οποίος δύναται εν ευρεία να διαγνωστεί ως υπεύθυνος επεξεργασίας[16].

IV. ΟΙ ΒΑΣΙΚΟΤΕΡΕΣ ΠΡΟΚΛΗΣΕΙΣ

1. Η οριοθέτηση της έννοιας των δεδομένων

Η έννοια των «προσωπικών δεδομένων» είναι κεντρική για τον ΓΚΠΔ και αποτελεί εν πολλοίς το υλικό του αντικείμενο (άρθρο 4)[17]. Επί της ουσίας, για να τυγχάνει εφαρμογής ο Γενικός Κανονισμός, τα συστήματα, οι πλατφόρμες, οι τεχνολογίες πρέπει να προβαίνουν σε κάποιου είδους επεξεργασία προσωπικών δεδομένων εντός του ορισμένου από τον Κανονισμό γεωγραφικού χώρου, δηλαδή της ΕΕ. Οι επίμαχοι τύποι δεδομένων που θα μας απασχολήσουν στα συστήματα κατανεμημένου καθολικού γενικώς αφορούν σε: α) Δεδομένα των συμμετεχόντων και των επαληθευτών στο σύστημα και β) άλλα δεδομένα, τα οποία σχετίζονται με ή περιλαμβάνονται στις συναλλαγές που εκτελούνται επί του συστήματος.

Στα συστήματα κατανεμημένου καθολικού, τα οποία βασίζονται στην τεχνολογία blockchain, ουσιαστικά πρέπει να ακολουθηθεί εκ νέου η τεχνική κατηγοριοποίηση, η οποία αποπειράθηκε ανωτέρω για να προσαρμοστεί η ανάλυση ειδικότερα στις ανάγκες των διαφοροποιημένων συστημάτων. Υπενθυμίζεται σε αυτό το σημείο ότι μια φορμαλιστική προσέγγιση δεν θα απέδιδε ως προς την κανονιστική θεώρηση των blockchains, μιας και τα τελευταία αυτονομούνται από τη νόρμα και μπορεί να υιοθετούν διαφοροποιημένους κανόνες και πρωτόκολλα μεταξύ τους. Η θεωρητική προσέγγιση είναι πάντοτε χρήσιμη στον ερμηνευτή, ωστόσο η τελική απόφαση και στάθμιση θα πρέπει πάντοτε να γίνεται *in concreto,* λαμβάνοντας υπόψιν τις επιμέρους περιστάσεις και δομές των συστημάτων.

Από τη μία, στα μη δημόσια συστήματα, τα οποία περιορίζουν την πρόσβαση μόνο σε ορισμένους προκαθορισμένους χρήστες, τα δεδομένα των χρηστών είναι παρόμοια με όσα αποθηκεύονται σήμερα από τις διάφορες πλατφόρμες. Συνεπώς, οι χρήστες είναι ορισμένοι ή έστω

[16] M. Berberich/M. Steiner, *Blockchain Technology and the GDPR, How to Reconcile Privacy and Distributed Ledgers*, European Data Protection Law Review, 3/2016, σελ. 423.

[17] Για τον ορισμό και την έννοια των προσωπικών δεδομένων, βλ. Α. Γέροντα, *Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων*, 2002, σελ. 15 επ. και Φ. Παναγοπούλου-Κουτνατζή, *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ*, 2017.

οριστοί συνήθως κατά όνομα, διεύθυνση e-mail, διεύθυνση IP, ενώ συμμετέχοντας στο σύστημα κοινοποιούν τα προσωπικά τους κλειδιά (δημόσιο και ιδιωτικό) και το ιστορικό συναλλαγών, το οποίο πάντοτε θα είναι δημόσιο. Ιδίως σε περιπτώσεις blockchain επενδυτικού περιεχομένου, στις οποίες οι χρήστες μπορούν να λάβουν συγκεκριμένα περιουσιακά στοιχεία, όπως ακίνητα, μετοχές ή ομόλογα, τα διάφορα κράτη ενδέχεται να επιβάλλουν τη λειτουργία κεντρικών αποθετηρίων/μητρώων (*Registerführer*), στα οποία οι χρήστες αποθηκεύονται ως προς τα προσωπικά τους δεδομένα και συνδέονται με το περιουσιακό στοιχείο ή τον τίτλο[18]. Σε αυτά τα blockchains δεν καταλείπεται αμφιβολία εκπλήρωσης του υλικού πεδίου εφαρμογής του ΓΚΠΔ ως προς την έννοια των δεδομένων.

Αντιθέτως, αμφιβολία γεννάται ως προς τα ανοιχτά και ελευθέρως προσβάσιμα blockchains, στα οποία τηρείται κρυπτογραφημένο το αρχείο των συναλλαγών και τα κλειδιά των χρηστών που συμμετέχουν, καθώς και διάφορες χρονολογικές πληροφορίες. Το αρχείο συναλλαγών περιλαμβάνει διάφορες πληροφορίες με κρυπτογραφημένη μορφή, όπως οικονομικά δεδομένα, ονόματα, διευθύνσεις των χρηστών, διευθύνσεις IP, ακόμη και ευαίσθητα προσωπικά δεδομένα, φυσικά κρυπτογραφημένα ή hashed[19]. Υπενθυμίζεται ότι οι χρήστες καθαυτοί αναγνωρίζονται ως μια αλφαριθμητική σειρά στο σύστημα, γεγονός που αποτρέπει την άμεση ταυτοποίησή τους από όσους έχουν πρόσβαση στα δεδομένα, ακόμη και από τα αντισυμβαλλόμενα μέρη στις διάφορες συναλλαγές τους, ενώ τα δεδομένα τηρούνται κρυπτογραφημένα και ασφαλή με την παροχή των δύο προσωπικών κλειδιών στον χρήστη. Υπό αυτή την έννοια, τα φυσικά πρόσωπα–κάτοχοι των αντίστοιχων λογαριασμών δεν είναι βέβαιο ότι θα μπορούσαν να ταυτοποιηθούν άμεσα μέσω αυτών των δεδομένων, εκτός αν τα ίδια επέλεγαν να κοινοποιήσουν τα κλειδιά αυτά. Επανέρχεται, επομένως, σε αυτό το σημείο η συζήτηση για το ποια δεδομένα δύνανται να ταυτοποιήσουν ένα πρόσωπο[20]. Η νομολογία *Breyer v Germany*[21] σχετικά με τις διευθύνσεις IP υπήρξε σε αυτό το σημείο καθοριστική και διόγκωσε το πεδίο εφαρμογής του ΓΚΠΔ έτι περαιτέρω.

Υπενθυμίζεται, σε κάθε περίπτωση, ότι στο άρθρο 29 του Opinion Paper τονίζεται ότι το hashing εμπίπτει ρητά στον Γενικό Κανονισμό, και τούτο διότι το hashing ουσιαστικά είναι μέθοδος ψευδωνυμοποίησης[22], όπως ακριβώς στην περίπτωση των blockchains, υπό την έννοια ότι η ταυτοποίηση υποκειμένων επεξεργασίας κατά το άρθρο 4 του ΓΚΠΔ είναι νοητή μόνον σε συνάρτηση και με άλλα δεδομένα, όπως εκείνα που επιπρόσθετα συλλέγονται και αποθηκεύονται

[18] Τούτο εισήχθη ιδίως στη Γερμανία με τον νόμο eWpG (γερμανικά: *Elektronische Wertpapieregesetz*) τον Αύγουστο του 2021, ο οποίος αποϋλοποίησε διάφορα αξιόγραφα, για παράδειγμα τα ομόλογα και τις μετοχές.

[19] P. Pesch/R. Böhme, *Datenschutz trotz öffentlicher Blockchain?,* Datenschutz und Datensicherheit, 2/2017, σελ. 94-95.

[20] Κατ' ακριβή διατύπωση του άρθρου 4 του ΓΚΠΔ: «*1) «δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου*».

[21] ΔΕΕ C-582/14, *Breyer κατά Γερμανίας*, 19.10.2016, ECLI:EU:C:2016:779.

[22] Για πλήρη ανάλυση της νομικής μεταχείρισης των ψευδωνυμοποιημένων δεδομένων, βλ. M. Mourby/E. Mackey/M. Elliot/H. Gowans/S.E Wallace/J. Bell/H. Smith/S. Aidinlis/J. Kaye, *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK*, Computer Law & Security Review, 34/2018 No. 2, σελ. 222-223.

στην αλυσίδα. Μέσω αλγορίθμων και επάλληλης συμμετοχής σε διάφορες αλυσίδες ταυτόχρονα μπορεί να ταυτοποιηθεί η οικονομική δραστηριότητα του χρήστη, οι επενδυτικές κινήσεις του, η διαχείριση των οικονομικών συναλλαγών και κατ' επέκταση η αξιοπιστία του.

Αφού διαγνωστεί ότι όντως τα συστήματα κατανεμημένου καθολικού σχετίζονται με δεδομένα χρηστών κατά την έννοια του άρθρου 4 ΓΚΠΔ, θα πρέπει ως αναγκαία συνέχεια να αναζητηθεί η μορφή της επεξεργασίας που εκτελείται. Είναι προφανές, έστω από ένα θεωρητικό πρίσμα, ότι η επεξεργασία στα blockchains γίνεται με αυτοματοποιημένα μέσα, το πρώτον με τη λήψη των εν λόγω δεδομένων, και έπειτα κάθε φορά που οι συναλλαγές δίδονται προς έγκριση αποθηκεύονται ως προς τα επιμέρους στοιχεία τους (πιθανότατα και εγγράφων) από τους χρήστες που έχουν πρόσβαση στους προσωπικούς τους υπολογιστές[23]. Κατόπιν, η διαδικασία της προσθήκης νέων συναλλαγών στην αλυσίδα απαιτεί επίσης την επεξεργασία των δεδομένων, με την έννοια της χρησιμοποίησης δημόσιων κλειδιών και των ψηφιακών υπογραφών των χρηστών για την επαλήθευσή τους.

Προφανώς, κατά μία έννοια και σε έναν βαθμό, οι χρήστες έχουν παραχωρήσει τη συναίνεσή τους κατά το άρθρο 6 παρ. 1 ως νομιμοποιητική αιτία για την εν λόγω επεξεργασία ως προς τις συγκεκριμένες συναλλαγές. Η συναίνεση αυτή δίδεται με την προσχώρηση και εγγραφή στο σύστημα, συνήθως μέσω αποδοχής των Γενικών Όρων Συναλλαγής ή της Σύμβασης Χρήστη. Αμφιβολίες εγείρονται εν προκειμένω ενόψει δύο παραγόντων: (α) Η επεξεργασία δεδομένων στο blockchain δεν σταματά εκεί που τελειώνει η κάθε συναλλαγή, αλλά τα δεδομένα συλλέγονται, αποθηκεύονται και επαναχρησιμοποιούνται για επαλήθευση συναλλαγών και hashing μέσω του συστήματος. Μάλιστα, με βάση την τεχνική δομή του συστήματος, τα δεδομένα θα επεξεργάζονται στο διηνεκές για όσο το blockchain υφίσταται, στον βαθμό που τα δεδομένα του ενός block συνδέονται λειτουργικά με την αξία/ταυτότητα του επόμενου block. Συνεπώς, προκειμένου να αναπτυχθεί η αλυσίδα, τα δεδομένα, ή ακριβέστερα η αξία hashing του συστήματος θα αναπαράγεται αναλλοίωτη, ενώ η διακοπή της και η αφαίρεση ενός block θα υπέσκαπτε την αλυσίδα από το σημείο εκείνο και έπειτα. Τούτο λόγω της ενεργοβόρου φύσεως του blockchain θα ήταν απαγορευτικό από άποψη κόστους και θα αλλοίωνε όλα τα μεταγενέστερα δεδομένα που αποθηκεύτηκαν στο σύστημα. (β) Ακραιφνής αρχή του ΓΚΠΔ είναι ότι το υποκείμενο επεξεργασίας δύναται να ανακαλέσει τη συναίνεσή του ανά πάσα στιγμή[24], κάτι που δεν φαίνεται να είναι εφικτό στα συστήματα blockchain. Η ανάκληση της συναίνεσης φυσικά δεν βλάπτει την επεξεργασία που εκτελέστηκε καθόσον υπήρξε συναίνεση, αλλά σαφώς δρα *ex nunc* για επεξεργασία που θα εκτελεστεί μελλοντικά. Σχετικά με την ανάκληση, η τελευταία αποτελεί δήλωση βούλησης, την οποία το υποκείμενο επεξεργασίας πρέπει να γνωρίζει ακριβώς σε ποιον να στρέψει προκειμένου αυτή να παράγει έννομα αποτελέσματα. Επανέρχεται, λοιπόν, το ζήτημα του προσώπου που συνιστά τον υπεύθυνο επεξεργασίας.

2. Η αναγνώριση του υπεύθυνου επεξεργασίας

Όλο το οικοδόμημα του Κανονισμού επαφίεται στην ύπαρξη ενός υποκειμένου, του υπεύθυνου επεξεργασίας, ο οποίος διαβεβαιώνει ότι τηρούνται οι διατάξεις του ΓΚΠΔ και εξοπλίζεται με

[23] Βλ. M. Artzt/L. Determann/W. Long, «Chapter 5: Blockchain and Data Privacy», ό.π., σελ. 198-199.
[24] Άρθρο 7 παρ. 3 του ΓΚΠΔ.

αδιαπραγμάτευτες εγγυήσεις ανεξαρτησίας και ουδετερότητας, με σαφή απαγόρευση περί λήψης εντολών[25]. Είναι εκείνα, το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας (ευρεία διατύπωση) που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα[26].

Προκειμένου έτσι να εφαρμοστεί αποτελεσματικά ο ΓΚΠΔ, πρέπει να επικρατεί σαφήνεια ως προς το ποιος φέρει τις ιδιότητες που απαιτούνται από τον νόμο στο άρθρο 4 παρ. 7, ιδιαίτερα τους ρόλους του «υπευθύνου επεξεργασίας» ή/και του «εκτελούντος την επεξεργασία». Μόνο εφόσον αυτές οι ιδιότητες είναι επαρκώς ορισμένες, τα υποκείμενα δικαίου μπορούν να ικανοποιηθούν ως προς τα δικαιώματα που τους χορηγούνται από τον ΓΚΠΔ και να στραφούν κατά συγκεκριμένων προσώπων. Σε αυτό το σημείο, πρέπει να επισημανθεί η ratio του ενωσιακού νομοθέτη να διατηρήσει διευρυμένη την έννοια του «υπευθύνου επεξεργασίας», περιλαμβάνοντας ως πιθανούς υπευθύνους κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, που κατά μόνας ή από κοινού προβαίνουν σε επεξεργασία προσωπικών δεδομένων. Η διατύπωση αυτή θεωρείται επιβεβλημένη εν όψει των ραγδαίων τεχνολογικών εξελίξεων και επιβεβαιώνει εν πολλοίς το δυναμικό πνεύμα του διατάξεων του ΓΚΠΔ. Η αλήθεια είναι ότι ακόμη και στη διαδικτυακή εποχή του *Web 2.0* (*peer-to-peer economy*), τα προβλήματα της οποίας κλήθηκε να λύσει ο ΓΚΔΠ, πολλάκις ελλοχεύουν προβλήματα και τα όρια είναι θολά ως προς την ταυτοποίηση του υπευθύνου επεξεργασίας. Στο σημείο αυτό πρέπει να επισημανθεί ότι ο υπεύθυνος επεξεργασίας ορίζεται ως προς την κάθε μεμονωμένη επεξεργασία δεδομένων, γεγονός που απαιτεί μια ad hoc κρίση και τεκμηρίωση των τεχνικών και πραγματικών παραγόντων που οδηγούν σε αυτήν[27]. Διαπιστώνεται, επομένως, από τη μία ότι ο ΓΚΠΔ προσπαθεί να αναγνωρίσει κεντρικές οντότητες φέρουσες τον έλεγχο για επεξεργασία δεδομένων και να τους απονείμει την αντίστοιχη ευθύνη. Από την άλλη, ως αποκεντρωμένες βάσεις δεδομένων, τα blockchain συστήματα, και ιδίως τα δημόσια και ελευθέρως προσβάσιμα, επιχειρούν να πετύχουν αυτή την αποκέντρωση αντικαθιστώντας την ύπαρξη κεντρικού μοντέλου με διασπορά σε περισσότερους χρήστες, συναπόφαση για επεξεργασία και προφανώς από κοινού ευθύνη. Πάντως ως προς το νομιμοποιητικό στοιχείο του άρθρου 4 παρ. 7, ο Κανονισμός φροντίζει να μην επιφυλάξει εξαιρέσεις· ακόμη και μεμονωμένα φυσικά πρόσωπα μπορεί να αποτελέσουν υπεύθυνους επεξεργασίας κατά την έννοια του νόμου[28].

Κατά γενική ομολογία, ωστόσο, ο ΓΚΔΠ είναι σχεδιασμένος για καταλογισμό παραβιάσεων σε συστήματα που παρουσιάζουν κέντρα εξουσίας, συνεπώς κεντρικές, συγκεντρωμένες δομές με ορισμένη διοίκηση και κάθετη ιεραρχία, ώστε οι σχέσεις και οι ιδιότητες να είναι οριστές ή έστω οριστέες. Η τεχνολογία blockchain, το πρώτον, δυναμίτισε αυτή την ισορροπία. Σε αυτό το σημείο, η διάκριση μεταξύ δημόσιων και ιδιωτικών blockchain συστημάτων παράγει εμφανή διαφοροποίηση στη νομική τους μεταχείριση[29]. Τα ιδιωτικά και περιορισμένης ορατότητας συστήματα προσιδιάζουν στις εταιρικές κάθετες συμβατικές δομές και έτσι θα τύχουν ίδιας μεταχείρισης με τις εταιρίες στο P2P μοντέλο οικονομίας. Σε αυτά εντοπίζεται ξανά μια κεντρική δομή ή κεντρικές δομές ασκούσες έλεγχο και καθορισμό της υφής των μέσων και των σκοπών επεξεργασίας. Αυτή η δομή θα είναι

[25] Β. Σωτηρόπουλος, *Υπεύθυνος Προστασίας Δεδομένων*, 2017, σελ. 44.
[26] Άρθρο 4 παρ. 7 ΓΚΠΔ.
[27] Βλ. EPRS, *Blockchain and the General Data Protection Regulation,* ό.π., σελ. 37.
[28] ΔΕΕ C-25/17, *Jehovah's witnesses*, ECLI:EU:C:2018:551, παρ. 75.
[29] Βλ. M. Berberich/M. Steiner, *Blockchain Technology and the GDPR*, ό.π., σελ. 424.

είτε το ίδιο το νομικό πρόσωπο που δημιούργησε την τεχνική υποδομή της πλατφόρμας, κατ' επέκτασιν οι ιδρυτές, είτε θα θεμελιώνεται συλλογικός έλεγχος (*joint controllership*)[30] ορισμένων χρηστών που τους αποδίδεται το προστιθέμενης αξίας προνόμιο να καθορίζουν τη φύση των δεδομένων που θα αποθηκεύονται στο blockchain ή/και να επηρεάζουν τις ροές δεδομένων. Για παράδειγμα, στα blockchain τα οποία διαχειρίζεται ένα κονσόρτιο ή πολλά κονσόρτια επιχειρήσεων, συνήθως υπάρχει σαφής υπόδειξη του υπευθύνου επεξεργασίας. Σε κάθε περίπτωση, δεν γεννάται αμφιβολία ως προς την ταυτότητα του υπεύθυνου επεξεργασίας και συνεπώς υπάρχει ευκρίνεια σε ζητήματα που άπτονται θέματα καταλογισμού ευθύνης[31].

Από την άλλη, τα δημόσια και ελευθέρως προσβάσιμα blockchains, για παράδειγμα το Bitcoin ή το Ethereum, περιλαμβάνουν και δομούνται επί τη βάσει μιας αποκεντρωμένης διακυβέρνησης κοινής ή συλλογικής συναίνεσης, με τους χρήστες να συνδράμουν ενεργά στην εξέλιξη του συστήματος και στη λήψη των αποφάσεων. Σε αυτά τα συστήματα, δεν υπάρχει μία οντότητα στην οποία να μπορεί να καταλογιστεί απόφαση για την επιλογή λογισμικού, ενημερώσεων ή την επιλογή τρόπου και μέσων επεξεργασίας. Το ζήτημα του καταλογισμού ευθύνης γίνεται πιο εμφανές στα εν λόγω, καθώς μια εσφαλμένη οριοθέτηση των ασκούντων έλεγχο θα μπορούσε, από τη μία, να οδηγήσει σε υπερδιεύρυνση του κύκλου των φερόντων ως υπευθύνων ή, από την άλλη, σε συρρίκνωσή τους. Και οι δύο προοπτικές αυτές θα χαρακτηρίζονταν από ανεπιεική αποτελέσματα.

Για να έχει κανείς μια ολική εικόνα και άποψη περί των ασκούντων έλεγχο επί των προσωπικών δεδομένων, πρέπει να διέλθει από το στάδιο της ανάλυσης των εκατέρωθεν συμφερόντων που κατά κανόνα αναπτύσσονται και συνυπάρχουν σε ένα οικοσύστημα ανοιχτού blockchain. Η χαρτογράφηση και ο συνυπολογισμός των ομάδων αντικρουόμενων συμφερόντων καταλήγει στο αποτέλεσμα της απόφασης των υπέρτερων συμφερόντων σε κάθε προκειμένη περίπτωση. Τα συμφέροντα αυτά περιλαμβάνουν τα συμφέροντα των ιδρυτών/προγραμματιστών, των επαληθευτών συναλλαγών/miners και των χρηστών. Να σημειωθεί ότι η ανάλυση αυτών των συμφερόντων αφορά το επίπεδο της υποδομής, δηλαδή το λειτουργικό σύστημα του blockchain καθαυτό (*Blockchain 1.0*), το οποίο κατόπιν μπορεί να χρησιμοποιηθεί ως υποδομή για περαιτέρω εφαρμογές και στρώματα επεξεργασίας (*Blockchain 2.0*). Στα στρώματα αυτά, υπεύθυνες είναι οι εκάστοτε επιχειρήσεις που δραστηριοποιούνται και παρέχουν την εν λόγω υπηρεσία.

Οι *ιδρυτές/προγραμματιστές* επί της ουσίας είναι οι δημιουργοί του blockchain, οι οντότητες εκείνες που είναι υπεύθυνες για τον σχεδιασμό του συστήματος, τις ενημερώσεις, την επιλογή των κανόνων και του πρωτοκόλλου συναίνεσης (White Paper). Κανείς θα μπορούσε να ισχυριστεί ότι η ομάδα αυτή διαθέτει το καταλυτικό πλεονέκτημα της τεχνικής γνώσης και της θέσης των κανόνων εντός του οικοσυστήματος. Ωστόσο, μετά τη δημιουργία και τη θέση του σε ισχύ, απολύουν κάθε είδους έλεγχο επί του οικοσυστήματος και δεν είναι σε θέση να καθορίσουν αν επί της ουσίας οι αλλαγές και οι κανόνες του πρωτοκόλλου θα ενσωματωθούν τω όντι στο σύστημα· αυτό ανήκει στην αρμοδιότητα των χρηστών ή των επαληθευτών των συναλλαγών. Οσάκις ένας προγραμματιστής προτείνει μια αλλαγή, το σύστημα το οποίο εκφεύγει του ελέγχου του καλείται να αποφασίσει αν θα την αποδεχτεί ή όχι. Συνεπαγομένου, ένας προγραμματιστής/ιδρυτής blockchain μόνο σε σπάνιες περιπτώσεις θα μπορούσε να θεωρηθεί υπεύθυνος επεξεργασίας, καθώς μόνη αρμοδιότητά του

[30] Άρθρο 26 του ΓΚΠΔ.

[31] Βλ. EPRS, *Blockchain and the General Data Protection Regulation,* ό.π., σελ. 43.

είναι η εξέλιξη του δικτύου και όχι η αποφασιστική αρμοδιότητα. Ωστόσο, οι προγραμματιστές έχουν μια επιπρόσθετη λειτουργία, την ανάπτυξη και παροχή των τεχνικών λύσεων που παρουσιάζουν συμβατότητα με το λειτουργικό της αλυσίδας και έτσι είναι αξιοποιήσιμες από τους επαληθευτές/miners κατά την εκτέλεση των καθηκόντων τους. Ως εκ τούτου, παρέχουν κατά μία έννοια τα μέσα της επεξεργασίας, τα οποία είναι τεχνολογικώς διαθέσιμα στις άλλες ομάδες συμμετεχόντων.

Σε αντίθεση με τους ιδρυτές, οι *επαληθευτές των συναλλαγών/miners*[32] θα μπορούσαν να εμπίπτουν στον όρο του υπευθύνου επεξεργασίας υπό μία έννοια. Ειδικότερα, η ομάδα αυτή ασχολείται κυρίως με την επαλήθευση των συναλλαγών που προτείνονται από τους χρήστες και την προοδευτική τους προσθήκη στην αλυσίδα ατέρμονων συνεχόμενων συναλλαγών, το chain. Οι επαληθευτές επίσης αποφασίζουν υπέρ της χρήσης του ενός ή του άλλου λογισμικού ή πρωτοκόλλου συναίνεσης και έχουν τοιουτοτρόπως καίρια θέση στο σύστημα, καθώς είναι εκείνοι που χειρίζονται τα μέσα επεξεργασίας των δεδομένων, χωρίς να ορίζουν ωστόσο τα ίδια και τους σκοπούς της επεξεργασίας. Για παράδειγμα, σε ένα Proof of Work οικοσύστημα οι miners επιλέγουν τον εξοπλισμό και τα λογισμικά που τους συμφέρουν για αποτελεσματικότερο mining κατόπιν προτάσεως των ιδρυτών, δεν επιλέγουν ωστόσο για ποιους σκοπούς τα εν λόγω δεδομένα θα αποθηκεύονται στην αλυσίδα[33]. Κατά αυτή την έννοια, θα μπορούσαν να εκπληρώνουν τον όρο των «ασκούντων την επεξεργασία», αλλά όχι και των υπευθύνων επεξεργασίας. Βεβαίως, θα μπορούσε κανείς να ισχυριστεί ότι η κυριαρχία επί της τεχνικής υποδομής και ο έλεγχος της αλυσίδας με την έννοια του καθορισμού της προσθήκης δεδομένων στο chain ενδεχομένως ισοδυναμεί με έναν *de facto* καθορισμό και των σκοπών επεξεργασίας των δεδομένων αυτών. Παρόμοια θέση τονίστηκε στη νομολογία μέσω της υπόθεσης *SWIFT*[34], στην οποία κρίθηκε ότι η ομώνυμη εταιρία, φερόμενη ως ασκούσα την επεξεργασία, δρούσε ως *de facto* υπεύθυνη επεξεργασίας μέσω έμμεσου καθορισμού των σκοπών επεξεργασίας των υποκειμένων[35]. Τούτο αποσυνδέει λειτουργικά τους φερόμενους ως υπευθύνους μέσω συμβολαίων και συμβάσεων με τους τω όντι επεξεργάζοντες τα δεδομένα, δημιουργώντας αποκλίσεις στη φορμαλιστική προσέγγιση του ΓΚΠΔ. Παρόμοια αναλογική νομολογιακή θεμελίωση και εφαρμογή θα μπορούσε να υποστηριχθεί και στην περίπτωση των blockchain συστημάτων. Οι επαληθευτές ενδέχεται εκ πρώτης όψεως να διαθέτουν ορισμένες και ρητές από το White Paper[36] του κάθε blockchain αρμοδιότητες, ωστόσο

[32] Ο όρος «επαληθευτές» ανταποκρίνεται στην ομάδα εκείνη που είναι υπεύθυνη για την επαλήθευση συναλλαγών και στα Proof of Work και στα Proof of Stake πρωτόκολλα συναίνεσης. Αντιθέτως, ο όρος «miners» απαντάται μόνο στα Proof of Work οικοσυστήματα και πάλι σχετίζεται με την επαλήθευση των συναλλαγών και την προοδευτική ανάπτυξη της αλυσίδας.

[33] Article 29 Data Protection Working Party, Opinion 1/2010, link, (τελευταία πρόσβαση 11.08.2022).

[34] ΔΕΕ C-350/10, *Nordea Pankki Suomi Oyj*, 28.07.2011, ECLI:EU:C:2011:532.

[35] Αναφορά στη νομολογία SWIFT εκπονείται και από το Data Protection Working Party, Opinion 3/2013, link, σελ. 9, (τελευταία πρόσβαση 11.08.2022).

[36] Το White Paper περιέχει τους κανόνες λειτουργίας του κάθε blockchain και διαμορφώνεται το πρώτον από τους ιδρυτές του. Σε δεύτερο επίπεδο, κάθε χρήστης και επαληθευτής, προκειμένου να συμμετέχει στο σύστημα, οφείλει να αποδεχτεί πριν την είσοδό του τους κανόνες του White Paper. Συνήθως σε αυτό ορίζονται τα οργανωτικά και λειτουργικά ζητήματα, όπως λόγου χάριν οι απαραίτητες πλειοψηφίες για τη λήψη των αποφάσεων, οι αμοιβές των επαληθευτών, ο όγκος των πληροφοριών που αποθηκεύονται στο block, οι κανόνες εισόδου και εξόδου μελών, κ.ά. Στα δημόσια blockchains, το White Paper μπορεί να τροποποιηθεί συνήθως με τη συμφωνία του 50+1% των full nodes (συνήθως των επαληθευτών) που συμμετέχουν στο σύστημα, ωστόσο οι ιδρυτές είναι ελεύθεροι να ορίσουν και διαφορετικά ποσοστά.

επί της ουσίας βρίσκονται στον έλεγχο των μέσων επεξεργασίας, και κάτι παραπάνω· ιδίως εν όψει των προηγμένων τεχνολογικών γνώσεων που διαθέτουν και της δυνατότητας να διχοτομήσουν την αλυσίδα σε περίπτωση λειτουργικής σύγκρουσής τους (*forking*)[37], ενδέχεται να έχουν το στρατηγικό πλεονέκτημα του έμμεσου καθορισμού των σκοπών συλλογής και επεξεργασίας των δεδομένων (*Control stemming from factual influence*)[38].

Η κρατούσα θεωρητικά άποψη[39], παρόλα αυτά, φέρει ως υπευθύνους επεξεργασίας του blockchain τους *χρήστες* του. Οι χρήστες έχουν τη λειτουργική δύναμη να ορίσουν την ποιότητα των δεδομένων που συλλέγονται και τα μέσα να ξεκινήσουν τη διαδικασία της επεξεργασίας: Ειδικότερα, οι χρήστες υπογράφουν συμβάσεις και υποβάλλουν προς έλεγχο συναλλαγές στους επαληθευτές. Κατά αυτό τον τρόπο οι χρήστες είναι εκείνοι που υποκινούν το blockchain ως προς τη διαδικασία αποθήκευσης, υποβάλλουν τα δεδομένα τους, παραλαμβάνουν δεδομένα άλλων χρηστών και τοιουτοτρόπως υποδεικνύουν έμμεσα τον τρόπο και τον σκοπό επεξεργασίας. Στα δημόσια και ελευθέρως προσβάσιμα blockchains, ο κάθε χρήστης έχει την αξίωση και τη δυνατότητα να συναποφασίσει ποια δεδομένα θα αποθηκεύονται και για ποιους σκοπούς στο πλαίσιο της αλυσίδας. Ενδεχομένως, η δυνατότητά του αυτή τον καθιστά συλλογικά υπεύθυνο επεξεργασίας μαζί με τους υπόλοιπους χρήστες του blockchain. Συνεπώς, από τη μία, οι ιδρυτές του συστήματος ή όσοι ενδέχεται να συμμετέχουν ενεργητικά στη λειτουργία του, δεν μπορούν να θεωρηθούν data controllers. Από την άλλη, ενδεχομένως οι χρήστες να μπορούν[40].

Κατά τη γράφουσα, ωστόσο, θα ήταν ίσως επιπόλαιη η διαπίστωση ότι στα δημόσια και ελευθέρως προσβάσιμα blockchains, ο κάθε χρήστης που αποθηκεύει δεδομένα στον προσωπικό του υπολογιστή μπορεί να θεωρηθεί και υπεύθυνος ή έστω συνυπεύθυνος επεξεργασίας. Πρώτον, τούτο ενδεχομένως θα ενέπιπτε στην εξαίρεση του άρθρου 2 παρ. 2 του ΓΚΠΔ σχετικά με δεδομένα για «προσωπική ή οικιακή δραστηριότητα»[41] και έτσι θα εξέπιπτε του πεδίου εφαρμογής του Κανονισμού (*household exception*)[42]. Δεύτερον, όσο ελκυστική κι αν μοιάζει, η τελεολογία πίσω από αυτή τη θεώρηση δεν πρέπει να καταλήγει στην απόσυρση της ευθύνης που παράγεται από

[37] Το *forking* είναι ένα είδος «συνταγματικής επανάστασης» των χρηστών. Ουσιαστικά είναι η διακλάδωση της αλυσίδας που εκπονείται ως αντίδραση στην απόρριψη των συνταγματικών κανόνων του πρωτοκόλλου ή των αλλαγών που προτείνονται από το σύστημα.

[38] Βλ. M. Berberich/M. Steiner, *Blockchain Technology and the GDPR*, ό.π., σελ. 11.

[39] J. Bacon et al, *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, Richmond Journal of Law and Technology, 25/2018 No. 1, link, (τελευταία πρόσβαση 11.08.2022)· Link, παρ. 22, (τελευταία πρόσβαση 11.08.2022).

[40] A. Bharadwaj, *Blockchain and the Right to Be Forgotten*, University Law Journal, 11/2021 no. 1, σελ. 51.

[41] Απόφαση της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων υπ' αριθ. 4/2006 περί το περιεχόμενο της εξαίρεσης της οικιακής δραστηριότητας. Ωστόσο, βλ. ενδεικτικά αντίθετη νομολογία ΔΕΕ, C-101/01, *Bodil Lindqvist,* ECLI:EU:C:2003:596, στην οποία το ΔΕΕ έκρινε ότι η δυνατότητα πρόσβασης των πληροφοριών από έναν απεριόριστο αριθμό χρηστών (εν προκειμένω οι δυνητικοί χρήστες που είχαν πρόσβαση στο ημερολόγιο) δεν συμβιβάζεται με την εξαίρεση της οικιακής δραστηριότητας. Παρόμοια νομολογία και ΔΕΕ, C-73/07, *Tietosuojavaltuutettu κατά Stakunnan Markkinaporssi Oy, Satamedia Oy*, παρ. 43-45. ECLI:EU:C:2008:727. Για περαιτέρω πληροφορίες περί του περιεχομένου της οικιακής εξαίρεσης, βλ. P. Jougleux, *Ο ΓΚΠΔ και η εξαίρεση της οικιακής δραστηριότητας: Η αχίλλειος πτέρνα της προστασίας (σχολιασμός της απόφασης 22/2021 της Αρχής Προσωπικών Δεδομένων, 29/03/2022)*, Επιθεώρηση Δικαίου Πληροφορικής, 01/2022, link, (τελευταία πρόσβαση 09.10.2022).

[42] Υπέρ παρόμοιας θέσης φαίνεται να τάσσεται και η Γαλλική Αρχή Δεδομένων σε πρόσφατη έρευνά της, βλ. Commission Nationale Informatique et Libertés (September 2018), *Premiers Éléments d'analyse de la CNIL: Blockchain' 3*, link, (τελευταία πρόσβαση 01.08.2022).

μια τεχνολογία *by design* από τους ιθύνοντες σχεδιαστές στους επιμέρους χρήστες του συστήματος, όσο αποκεντρωμένες κι αν είναι οι μέθοδοι επεξεργασίας. Τούτο θα συνεπαγόταν το παράδοξο αποτέλεσμα να ενέχεται ο κάθε οικιακός χρήστης/επενδυτής που θα αναμειγνύονταν με το σύστημα μέσω αγοράς Bitcoin, να εκτίθετο και ως συνυπεύθυνος σε τεράστια ποσά αποζημίωσης για παραβάσεις του ΓΚΠΔ, χωρίς να έχει επίγνωση του γεγονότος της επεξεργασίας, πολλώ δε μάλλον ότι φέρει την ιδιότητα του υπεύθυνου επεξεργασίας.

Αντιθέτως, προκρίνεται από την παρούσα μελέτη η καθιέρωση ενός μέτρου ευθύνης από κοινού των ιδρυτών/προγραμματιστών και των επαληθευτών του συστήματος (*joint controllership*), σύμφωνα και με τα κριτήρια του ελέγχου των μέσων και των σκοπών της επεξεργασίας. Η διάγνωση από κοινού ευθύνης δεν πρέπει να συνεπάγεται και ίση ευθύνη για τους παράγοντες που συμμετέχουν στη διαδικασία. Αντιθέτως, κατά την πάγια νομολογία του ΔΕΕ πρέπει να γίνεται στάθμιση του μέτρου της ευθύνης για τους παράγοντες, σύμφωνα με το στάδιο συμμετοχής τους, τον βαθμό επιρροής τους στο σύστημα και τις εν γένει περιστάσεις της υπόθεσης[43].

3. Άρθρο 17 ΓΚΠΔ: Το δικαίωμα του υποκειμένου για διαγραφή των δεδομένων του

Από τα πιο αμφιλεγόμενα άρθρα του Γενικού Κανονισμού συνιστά το λεγόμενο δικαίωμα για διαγραφή των δεδομένων του υποκειμένου επεξεργασίας, ή άλλως και ευρύτερα γνωστότερο «δικαίωμα στη λήθη»[44], το οποίο σωματοποιείται στο άρθρο 17 του Γενικού Κανονισμού. Ήδη, στο σημείο 65 του Προοιμίου του Κανονισμού φανερώνεται η βούληση του Ενωσιακού νομοθέτη για άμεση κατοχύρωση του δικαιώματος του προσώπου για διαγραφή των δεδομένων του που δεν επιθυμεί να εκτίθενται δημόσια ή για τα οποία έχει εκλείψει ο σκοπός επεξεργασίας. Δυστυχώς, το περιεχόμενο του όρου «διαγραφή»[45] δεν είναι αποσαφηνισμένο και έτσι ο όρος παρουσιάζει συστηματικές δυσκολίες στην ερμηνεία καθαυτός. Η θέση της Ελληνικής Αρχής Προστασίας Δεδομένων επικεντρώνεται υπέρ της θεμελίωσης ενός γενικευμένου δικαιώματος διαγραφής, και όχι απαραίτητα λήθης[46]. Τούτο απέδειξε με την πρακτική της σε περιπτώσεις προσφυγών κατά της Google, κατά τις οποίες δέχτηκε μεν διαγραφή μέσω της κατάργησης των υπερσυνδέσμων που οδηγούν στην πηγή των πληροφοριών, όχι όμως και την απαλοιφή των πληροφοριών καθαυτών από την πλατφόρμα[47]. Παρόμοια πρακτική έχει ακολουθήσει και η Γαλλική Αρχή Προστασίας Δεδομένων.

Η νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (στο εξής: ΔΕΕ), στην Υπόθεση *Google Spain SL*[48], είχε τονίσει ήδη πριν τη θέση σε ισχύ του ΓΚΠΔ το δικαίωμα κάθε υποκειμένου για προσέγγιση του χειριστή μηχανής αναζήτησης (εν προκειμένω: η Google LLC, ισπανική θυγατρική

[43] Link, σελ. 19, (τελευταία πρόσβαση 09.10.2022).

[44] Οι δύο όροι χρησιμοποιούνται στην παρούσα μελέτη με κοινό περιεχόμενο, ωστόσο εννοιολογικά και δογματικά δεν είναι ταυτόσημοι. Για μια πραγματεία επί του εν λόγω δικαιώματος, βλ. Φ. Παναγοπούλου-Κουτνατζή, *Η Εξέλιξη του δικαιώματος στη λήθη*, ΕφημΔΔ, 6/2016, σελ. 714 επ.

[45] Σύμφωνα με το λεξικό του Μπαμπινιώτη, ο όρος διαγραφή στα Νέα Ελληνικά σημαίνει την «*ακύρωση της ύπαρξης ή της ισχύος*», link, σελ. 478. Ενώ αγγλιστί, ο αντίστοιχος όρος «*erasure*» ερμηνεύεται με βάση το Oxford English Dictionary ως «*the removal of writing, recorded material or data*», link.

[46] Βλ. Φ. Παναγοπούλου-Κουτνατζή, *Η Εξέλιξη του δικαιώματος στη λήθη*, ό.π., σελ. 720.

[47] Ενδεικτικά, βλ. Αποφάσεις της Ελληνικής Αρχής Προστασίας Δεδομένων υπ. αριθ. 82/2016, 83/2016, 84/2016.

[48] ΔΕΕ C-131/12, *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*, 13.05.2014, ECLI:EU:C:2014:317.

της Google) με αίτημα τη διαγραφή των προσωπικών δεδομένων του. Η μη ικανοποίηση ιδίως του αιτήματός του νομιμοποιεί την έγερση αξιώσεων για δικαστική προσφυγή εναντίον της εν λόγω μηχανής αναζήτησης[49]. Η απόφαση παρουσιάζει ερευνητική σημασία, καθώς επηρεάζει έναν πολύ σημαντικό παράγοντα του διαδικτύου, κυρίως την εταιρία Google (μηχανή αναζήτησης), ως υπεύθυνη επεξεργασίας δεδομένων, ωστόσο προχωράει και ένα βήμα παρακάτω· με την ευρεία οριοθέτηση της έννοιας της «επεξεργασίας» προσωπικών δεδομένων (ιδίως το *processing*), ανοίγει τον δρόμο για τη θεμελίωση απαιτήσεων για παραβάσεις του ΓΚΠΔ εναντίον πολλών παραγόντων που δραστηριοποιούνται στο διαδίκτυο, αναπόσπαστο μέρος των οποίων αποτελούν και τα συστήματα blockchain σήμερα. Ιδίως για τα δημόσια blockchains, στα οποία οι κρυπτογραφημένες πληροφορίες είναι διαθέσιμες στο ευρύ κοινό, θα πρέπει να λαμβάνονται ιδιαιτέρως σοβαρά παρόμοια αιτήματα των υποκειμένων. Χαρακτηριστικό παράδειγμα αποτελούν οι «έξυπνες συμβάσεις», οι οποίες κατά κύριο λόγο «τρέχουν» σε blockchain τύπου Ethereum.

Το ήδη περίπλοκο ζήτημα της διαγραφής δεδομένων που έχουν τεθεί στο διαδίκτυο εκτραχύνεται έτι περαιτέρω μέσω των τεχνολογιών κατανεμημένου καθολικού. Εκ πρώτης όψεως, με βάση τα προαναφερθέντα χαρακτηριστικά, οι δύο όροι (δικαίωμα στη λήθη και blockchain) φαίνονται λειτουργικά ασυμβίβαστοι. Ιδίως για τις ανοιχτές/δημόσιες και ελευθέρως προσβάσιμες κατηγορίες, δεν καταλείπεται περιθώριο μεταβολών ή διαγραφής, καθώς η εν λόγω αποτελεί μια τεχνολογία σχεδιασμένη να μην επιτρέπει εκούσια μεταβολές επί των αποθηκευμένων δεδομένων. Κατ' αυτό τον τρόπο επιτυγχάνεται η μετατόπιση της εμπιστοσύνης στο σύστημα, το οποίο διαφυλάσσει την ακεραιότητα και τη γνησιότητα των δεδομένων ως καταχωρήθηκαν. Άλλως, δεν θα μπορούσε ένα αποκεντρωμένο μοντέλο αποθήκευσης να είναι αποτελεσματικό και λειτουργικό, αφού ο κάθε χρήστης με κατάλληλο τεχνικό υπόβαθρο θα μπορούσε να μεταβάλλει την αλυσίδα των δεδομένων και να την επηρεάσει κατά βούληση με τη μέθοδο του *reverse engineering*. Το ζήτημα είναι αν μπορεί ο ερμηνευτής και ο νομοθέτης να συμβιβάσει της επιταγές της νέας τεχνολογίας με αξιώσεις προστασίας ανάλογες με του ΓΚΠΔ με δίκαιο τρόπο, χωρίς να θυσιάζει την καινοτομία στον βωμό της προστασίας ή της ασφάλειας και το αντίστροφο.

Κατόπιν της ανωτέρω ανάλυσης ανακύπτουν δύο καίρια ερωτήματα για τον ερμηνευτή του δικαίου, όταν καλείται να αποφασίσει για πρακτικές σε συστήματα blockchain: Το πρώτο εκ των δύο αφορά σε ένα διαδικαστικό/νομιμοποιητικό ζήτημα, και ιδίως στον αποδέκτη του αιτήματος για διαγραφή, με άλλα λόγια το πρόσωπο που θα αποτελεί έναν υπεύθυνο επεξεργασίας (data controller) σε συστήματα αποκεντρωμένης λειτουργικότητας. Τούτο το ερώτημα δεν είναι διόλου ευκαταφρόνητο, καθώς συνοδεύεται με προβληματικές νομιμότητας, ιδίως προληπτικά της τήρησης των αυξημένων επιταγών του νόμου για τους υπευθύνους επεξεργασίας, αλλά κατασταλτικά και καταλογισμού ευθύνης σε περίπτωση μη συμμόρφωσης με τις επιταγές του Κανονισμού.

Το δεύτερο –και ίσως κρισιμότερο ερώτημα– σχετίζεται με την ιδιότητα της τεχνολογίας blockchain να μην επιτρέπει διαγραφή ή τροποποίηση των στοιχείων που αποθηκεύτηκαν στην αλυσίδα, παρά μόνο με συμφωνία των μισών τουλάχιστον ενεργών συμμετεχόντων με πλήρη

[49] Για περισσότερες πληροφορίες σχετικά με την Απόφαση του ΔΕΕ, βλ. link, και E. Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, Human Rights Law Review, 14/2014, link, σελ. 761-777, (τελευταία πρόσβαση 05.08.2022).

δικαιώματα του δικτύου[50]. Μια θεωρητική προσέγγιση επιχειρεί να εισάγει τη λειτουργία των συστημάτων αυτών και την ανάγκη για μη διαγραφή των δεδομένων στην εξαίρεση του άρθρου 6 του ΓΚΠΔ: Υπό την προοπτική αυτή, οι λειτουργικές απαιτήσεις των συστημάτων blockchain δύνανται να εισαχθούν στη σύννομη επεξεργασία των δεδομένων κατά τις περιπτώσεις (β) ή (στ) του εν λόγω άρθρου[51]. Η θεωρητική αυτή άποψη παρουσιάζει ένα ενδιαφέρον, λαμβάνοντας υπόψιν την τεχνολογική ουδετερότητα του Κανονισμού, ωστόσο ο ερμηνευτής σε τέτοιες περιπτώσεις θα πρέπει πάντοτε να προβαίνει σε μια *in concreto* στάθμιση των εκατέρωθεν συμφερόντων, των κατ' ιδίαν περιστάσεων, όπως το μέγεθος και η σοβαρότητα της προσβολής, η συναίνεση που έχει δοθεί από τον χρήστη, η βλάβη, κ.ά. Είναι βέβαιο ότι η τεχνολογία δεν δύναται να εξικνείται στο σημείο εκείνο που να θίγονται τα προσωπικά δεδομένα των χρηστών και να χρησιμοποιηθεί για αυτό τον λόγο ως μέσο καταστρατήγησης των προστατευτικών διατάξεων. Μια γενικευμένη φορμαλιστική θεώρηση της τεχνολογίας ως εξαίρεση στον ΓΚΠΔ *de lege ferenda* ενδεχομένως ανοίγει την «πίσω πόρτα» για εισαγωγή κάθε νεωτερισμού στη διέξοδο αυτή, και άρα τη *de facto* καταστρατήγηση των διατάξεων του Γενικού Κανονισμού.

Η πρώτη λύση που έχει προκριθεί είναι η αποθήκευση των ευαίσθητων πληροφοριών *off-chain* ή *side-chain*, δηλαδή σε έναν συμβατικό, ανεξάρτητο server εκτός του βασικού blockchain, και η σύνδεσή τους μέσω *hashing* ενός *link* στη βασική αλυσίδα. Σε αυτή την περίπτωση, η λειτουργική σκοπιμότητα έγκειται στο ότι σε περίπτωση που το υποκείμενο επεξεργασίας αιτηθεί τη διαγραφή των δεδομένων του, η καταστροφή του υπερσυνδέσμου ουσιαστικά οδηγεί σε ανυπαρξία των δεδομένων στην αλυσίδα. Ο κάθε χρήστης που θα επιχειρεί να έχει πρόσβαση θα προσκρούει σε σφάλμα του υπερσυνδέσμου. Ωστόσο, η λύση αυτή δεν μπορεί να θεωρηθεί αξιόπιστη· πρώτον, η καινοτομία μένει αναξιοποίητη εφόσον τα δεδομένα και πάλι αποθηκεύονται σε κεντρικά pools, τα οποία ελέγχονται από ορισμένες εταιρίες. Δεύτερον, θα δημιουργείτο μεγάλη τεχνολογική ανασφάλεια, καθώς το σύστημα θα ήταν ευάλωτο σε πολλά σφάλματα: Συγκεκριμένα, το off ή side-chain σύστημα θα έπρεπε πάντα να διασφαλίζει συμβατότητα με όλες τις πιθανές εκδόσεις του blockchain και όλες τις μορφές ενημερώσεων που θα μπορούσαν να υιοθετήσουν οι χρήστες. Ειδάλλως, ο κίνδυνος μη συμβατότητας και απώλειας δεδομένων ή μη ορατότητας δεδομένων από χρήστες που φέρουν πιο πρόσφατες ή πιο παλαιές εκδόσεις του λογισμικού θα ήταν υπαρκτός. Τρίτον –και ίσως σοβαρότερο από όλα– είναι ότι ακόμη δεν έχει γίνει ευρέως αποδεκτό στη θεωρία και τη νομολογία ότι η καταστροφή και η απαλοιφή των συνδέσμων, και όχι των ίδιων των πηγών πληροφοριών, συνιστά «διαγραφή» κατά την έννοια του Γενικού Κανονισμού. Το περιεχόμενο του δικαιώματος στη λήθη δεν θα πρέπει να περιορίζεται στην καταστροφή μόνο των μέσων προς εύρεση των δεδομένων των ατόμων, εν προκειμένω των συνδέσμων, αλλά και στα ίδια τα δεδομένα των υποκειμένων, για τα οποία εκλείπει η νόμιμη αιτία της διατήρησης από τη μηχανή αναζήτησης. Ειδάλλως, θα ισοδυναμούσε αυτή η παραδοχή με αλλοίωση του περιεχομένου του

[50] Ακόμη και σε περίπτωση συναίνεσης της πλειοψηφίας των ενεργών χρηστών του συστήματος, θα ήταν απαγορευτικό το κόστος σε επίπεδο ενέργειας και υπολογιστικής ισχύος. Η συνεχόμενη αλυσίδα αποτελείται από κόμβους ενωμένους λειτουργικά μεταξύ τους, συνεπώς η διαγραφή ενός κόμβου θα απαιτούσε την αναδρομική λύση ολόκληρης της αλυσίδας και της αποθηκευμένης σειράς εγγραφών μέχρι την εγγραφή που πρέπει να διαγραφεί και έπειτα πάλι την αναδόμησή της. Περιττό να αναφερθεί ότι το κόστος εν προκειμένω θα καθίστατο απαγορευτικό και θα είχε τεράστιο περιβαλλοντικό αντίκτυπο.

[51] Βλ. M. Berberich/M. Steiner, *Blockchain Technology and the GDPR*, ό.π., σελ. 426.

δικαιώματος και μετατροπή του από ένα δικαίωμα «διαγραφής», με την έννοια της αφαίρεσης από τη σφαίρα του κοινώς προσβάσιμου, σε ένα δικαίωμα αφαίρεσης από μια λίστα αποτελεσμάτων αναζήτησης, τούτο που σωστά η θεωρία ονοματίζει delisting[52]. Σαφώς η ερμηνεία των διατάξεων του νόμου οφείλει να κάμπτει την ψυχρή αποτύπωση των λέξεων και των σημείων του κειμένου, ωστόσο η γραμματική ερμηνεία με την έννοια της συγκεκριμένης επιλογής των λέξεων από τον νομοθέτη δεν πρέπει να παραγκωνίζεται. Ενδεχομένως, μέσα από την ακριβή επιλογή των λέξεων και την ανάλογη δικαστική απόπειρα εμμονής στο ουσιαστικό τους περιεχόμενο αντανακλάται η ανάγκη όχι μόνο μιας ψευδεπίγραφης, αλλά μιας πιο ουσιαστικής και επικεντρωμένης προστασίας εν συνόλω· μιας προστασίας που θα διαφυλάσσεται μέσω της ικανότητας του ατόμου όχι μόνο να εξαφανίζει προσωρινώς, αλλά να εξαλείφει ολικώς το περιεχόμενο που άπτεται της ιδιωτικής σφαίρας του, ανεξαρτήτως τεχνολογικού μέσου[53].

Στην περίπτωση των blockchain, για να επανέλθει η ανάλυση στο αρχικό της περιεχόμενο, μια δεύτερη τεχνικά αποδεκτή λύση είναι η δημιουργία των λεγόμενων πολυδιάστατων blockchains (*multilayered blockchains*) προκειμένου να επιτευχθεί συμμόρφωση με τον ΓΚΠΔ. Σύμφωνα με αυτή τη λύση, τα δεδομένα θα εξάγονται από ένα ιδιωτικό blockchain και θα μεταφέρονται σε ένα δημόσιο blockchain. Τα δύο αυτά διακριτά blockchains ουσιαστικά διασφαλίζουν ότι τα δεδομένα θα υφίστανται πάντοτε στο ιδιωτικό blockchain, το οποίο θα είναι περιορισμένης πρόσβασης, και μόνο θα συνδέονται λειτουργικά με το δημόσιο, το οποίο είναι ορατό σε όλους[54].

Γενικά, στους όρους των blockchains (*White Papers*) ενδέχεται να μπορούν να εισαχθούν ρήτρες συναίνεσης όταν υποκείμενα αιτούνται τη διαγραφή, ώστε να υπάρχει υποχρεωτική συναίνεση της πλειοψηφίας των χρηστών για απόσυρση αυτών των δεδομένων. Το πρόβλημα με αυτή τη λύση είναι ότι στον πυρήνα της είναι ενεργοβόρα και απαγορευτική από άποψη κόστους, ωστόσο τηρεί τα μεγαλύτερα εχέγγυα φερεγγυότητας, προστασίας και ασφάλειας για τα υποκείμενα επεξεργασίας και τους χρήστες των blockchains. Παρόμοια ρήτρα με προειδοποιητική λειτουργία μπορεί να συμφωνηθεί και για τους κινδύνους που ενέχει η εγγραφή σε ένα ανοιχτό δίκτυο blockchain. Τέτοιες ρήτρες που αποστερούν τον ιδιώτη από τα εγγενή και νόμιμα δικαιώματά του ως μέρος των γενικών όρων συναλλαγής ενδεχομένως να κριθούν άκυρες από τα δικαιοδοτικά όργανα ως αιφνιδιαστικές και παράνομες κατά τις γενικές διατάξεις. Ωστόσο, θα μπορούσαν να αποτελούν περιεχόμενο χωριστής συμφωνίας, ενόψει και των τεχνικών χαρακτηριστικών των blockchains, το οποίο θα πρέπει να συμφωνηθεί ρητά από τους χρήστες ως προϋπόθεση για να εισέλθουν στην πλατφόρμα, μαζί με την πολιτική προστασίας προσωπικών δεδομένων και τους γενικούς όρους συναλλαγών.

Φυσικά παρόμοια προβληματική με αυτή που αναπτύχθηκε στο πλαίσιο του άρθρου 17 παρ. 1 για το δικαίωμα στη διαγραφή ανακύπτει και σε σχέση με το δικαίωμα του άρθρου 16 του ΓΚΠΔ, δηλαδή το δικαίωμα του υποκειμένου για τροποποίηση των δεδομένων του. Καθώς η προβληματική είναι κοινή, συνεπώς και οι λύσεις θα παρουσιάζουν παρόμοιο περιεχόμενο, οπότε για την οικονομία της παρούσας μελέτης δεν επαναλαμβάνονται σε αυτό το σημείο. Τούτο που πρέπει να τονιστεί χωριστά είναι ότι ενδεχομένως για κάποιες περιπτώσεις δεδομένων, το δικαίωμα αυτό μπορεί να ικανοποιηθεί με την εκ νέου δημοσίευση συμπληρωματικών δηλώσεων περί μίας

[52] Βλ. Φ. Παναγοπούλου-Κουτνατζή, *Η Εξέλιξη του δικαιώματος στη λήθη*, ό.π., σελ. 725.
[53] Ι. Ιγγλεζάκη, *Το δικαίωμα στη λήθη: Ένα νέο ψηφιακό δικαίωμα για τον κυβερνοχώρο*, διαθέσιμο στο link.
[54] Βλ. M. Artzt/L. Determann/W. Long, «Chapter 5: Blockchain and Data Privacy», ό.π., σελ. 224.

συναλλαγής με το σωστό τούτη τη φορά περιεχόμενο, χωρίς να απαιτείται ολοσχερής διαγραφή. Ωστόσο, αυτή η λύση είναι απρόσφορη για περιπτώσεις ευαίσθητων προσωπικών δεδομένων ή εγγράφων των χρηστών.

4. Blockchain και αρχή της αναλογικότητας

Το αντικατόπτρισμα της αρχής της αναλογικότητας στον ΓΚΠΔ γίνεται εμφανές και ρητό μέσω των προβλέψεων του Προοιμίου του, σκέψη 170, του άρθρου 5 παρ. 1 στ. (β) και (γ) μέσω των περιορισμών της συλλογής και επεξεργασίας των απολύτως αναγκαίων μόνον δεδομένων (*data minimization*) για τους απολύτως αναγκαίους, ρητούς, κοινοποιημένους και νόμιμους σκοπούς (*purpose limitation*)[55]. Οι δύο αυτές αρχές έχουν την ίδια κοινή καταβολή και εν πολλοίς αλληλοκαλύπτονται ως προς το πεδίο ορισμού τους. Συνεπώς, η συλλογή και επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται ενόψει νόμιμων προκαθορισμένων και γνωστών στο υποκείμενο επεξεργασίας σκοπών, ο τρόπος συλλογής δε πρέπει να είναι εύλογος, πρόσφορος και να μην βαίνει πέραν του αναγκαίου μέτρου. Στον ελληνικό χώρο η αρχή της αναλογικότητας καθιερωνόταν ήδη με το άρθρο 4 παρ. 1 εδ. β΄ του προϊσχύσαντος ν. 2472/1997 και είχε αποτυπωθεί σε πληθώρα αποφάσεων της Αρχής πριν από τη ρητή θέσπισή της στον Ευρωπαϊκό Κανονισμό[56].

Οι εν λόγω στα συστήματα κατανεμημένου καθολικού σχετίζονται: Το πρώτον, με το κατά πόσο τα δεδομένα που αποθηκεύονται κατόπιν της εκτέλεσης διάφορων συναλλαγών μπορούν ή πρέπει να υπόκεινται σε επεξεργασία και μετά το πέρας των σκοπών αυτών, δηλαδή της εκπλήρωσης των συναλλαγών. Το blockchain φύσει ασταμάτητα επεξεργάζεται τα δεδομένα για όσο αυτό υπάρχει, αφού αυτά εισέλθουν στο σύστημα. Σε συγκεκριμένες περιπτώσεις εκτελείται μια επεξεργασία κατόπιν της συναλλαγής του χρήστη, επειδή τα δεδομένα πλέον αποτελούν μέρος της αλυσίδας συναλλαγών για σκοπούς άλλους από τους οποίους δόθηκε η αρχική συναίνεση, δηλαδή καθ' υπέρβαση των σκοπών επεξεργασίας[57]. Δεύτερον, η αρχή σχετίζεται με το ποια δεδομένα πρέπει ακριβώς να συλλέγονται για τους εν λόγω σκοπούς και ο περιορισμός τους στα απολύτως αναγκαία για την επεξεργασία για τον απολύτως αναγκαίο χρόνο. Διαφαίνεται έτσι ότι η αρχή του περιορισμού των προς συλλογή δεδομένων (data minimization) έχει προσλάβει μια χρονική διάσταση, η οποία εκ νέου δυναμιτίζεται.

Η αρχή της αναλογικότητας, η οποία καθιερώνεται μέσω των δύο προαναφερθέντων αρχών, εγείρει το πάλαι ποτέ αίτημα της *privacy by design*, το οποίο σήμερα εμφανίζεται κανονιστικά στο άρθρο 25 του ΓΚΠΔ[58]. Το ζητούμενο σε αυτή την περίπτωση θα ήταν η αναζήτηση μιας συμμόρφωσης στον ΓΚΠΔ προληπτικά, και όχι κατασταλτικά, ξεκινώντας από τον ίδιο τον σχεδιασμό του λειτουργικού συστήματος[59]. Με βάση το άρθρο αυτό, οι υπεύθυνοι επεξεργασίας των blockchains θα πρέπει να είναι σε θέση να προβλέψουν και να σχεδιάσουν έτσι τη συλλογή και

[55] Βλ. Article 29 Data Protection Working Party, Opinion 1/2010, ό.π., σελ. 3, 4.

[56] Βλ. ενδεικτικά αποφάσεις της Ελληνική Αρχής Προστασίας Δεδομένων υπ. αριθ. 31/2004, 44/2007, 76/2013, 97/2012.

[57] Βλ. M. Artzt/L. Determann/W. Long, «Chapter 5: Blockchain and Data Privacy», ό.π., σελ. 222.

[58] Βλ. M. Berberich/M. Steiner, *Blockchain Technology and the GDPR*, ό.π., 425.

[59] Article 29 Data Protection Working Party, *The Future of Privacy* (1 December 2009) Working Paper 168 (02356/09/EN), link, σελ. 41-56, (τελευταία πρόσβαση 04.08.2022)· D. Schartum, *Making privacy by design operative*, International Journal of Law and Information Technology, 24/2016, σελ. 151-175.

αποθήκευση δεδομένων, ώστε αυτή να κατοχυρώνει συμμόρφωση στις επιταγές του Κανονισμού ήδη σε ένα πρώιμο στάδιο επιλογής των μέσων επεξεργασίας, παραδείγματος χάριν με περιορισμό των δυνατοτήτων συλλογής που προσφέρονται μέσα από το ίδιο το λειτουργικό σύστημα. Μια λύση θα μπορούσε, όπως και στο παράδειγμα του δικαιώματος στη λήθη, να συνιστά η *off-chain* αποθήκευση δεδομένων ή η χρήση πολυδιάστατων διασυνδεδεμένων συστημάτων, φυσικά με τις επακόλουθες επιφυλάξεις που αναλύθηκαν ανωτέρω. Θεωρητικά η διατήρηση δεδομένων σε blockchain μέσω ανωνυμοποίησής τους καθίσταται συμβιβάσιμη με τον ΓΚΠΔ, συνεπώς ενδεχομένως ένας διαχωρισμός των χρήσιμων για το σύστημα πληροφοριών και εκείνων που είναι περιττές κρίνεται αναγκαίος ήδη σε επίπεδο προγραμματισμού. Το βάρος επωμίζονται, ενδεχομένως προληπτικά, για άλλη μια φορά οι ιδρυτές του συστήματος και εκείνοι που ευθύνονται για την ανάπτυξη του κατάλληλου λογισμικού.

Η αλήθεια είναι ότι τα χαρακτηριστικά της τεχνολογίας κατανεμημένου καθολικού, όπως αυτά προς το παρόν προβάλλουν, εκ πρώτης όψεως δεν δείχνουν να συμμορφώνονται με τις επιταγές του άρθρου 25. Ωστόσο, το κατά πόσο το άρθρο 25 καθαυτό επιβάλλει συγκεκριμένες και οριστές υποχρεώσεις ή επαναλαμβάνει τη γενική υποχρέωση συμμόρφωσης με τις διατάξεις του ΓΚΠΔ είναι επίσης ένα θέμα που τυγχάνει ευρέος διαλόγου[60].

Μια ακόμη έκφανση της αρχής της αναλογικότητας αφορά στις περιπτώσεις διεθνούς μεταφοράς δεδομένων. Ο Κανονισμός για τα Προσωπικά Δεδομένα καθιερώνει μια γενική απαγόρευση μεταφοράς προσωπικών δεδομένων χρηστών σε χώρες εκτός της ΕΕ, με την εξαίρεση των χωρών εκείνων που η Ευρωπαϊκή Επιτροπή κρίνει ως κατάλληλες διότι διαφυλάσσουν επαρκές επίπεδο προστασίας (*standard of essential equivalence*). Τούτη είναι και η πάγια τοποθέτηση του ΔΕΕ στις περιπτώσεις διεθνούς μεταφοράς, όπως αυτή αποτυπώθηκε στην απόφαση *Schrems I*. Ουσιαστικά, με την εισαγωγή ενός προτύπου ισοτιμίας και σύγκρουσης των δικαιωμάτων ανοίγει η πίσω πόρτα για την εισαγωγή όλων των προβληματισμών αναλογικότητας που αυτές επισύρουν. Πράγματι, η αρχή της αναλογικότητας αποτελεί το ισχυρότερο εκείνο εργαλείο στάθμισης των εκατέρωθεν συμφερόντων, εντούτοις ο τρόπος ερμηνείας και εμφιλοχώρησής της ως προς το πώς θα ερμηνευτεί το «επαρκές και ισότιμο επίπεδο προστασίας» παραμένει αντικείμενο διαφωνίας στη θεωρία και τη νομολογία. Οι περιορισμοί της ΕΕ στη διεθνή μεταφορά δεδομένων εφαρμόζονται και στα συστήματα blockchain και μάλιστα εκτενέστερα, καθώς οι χρήστες είναι πολύ πιθανό να βρίσκονται σε χώρες εκτός ΕΕ. Το ζήτημα εδώ είναι πολυδιάστατο. Αφενός, είναι αποδεικτικής φύσεως. Στα δημόσια blockchains, είναι δυσχερές να αποδειχτεί ποια είναι η ακριβής τοποθεσία των χρηστών που εμπλέκονται στο σύστημα, συνεπώς το έργο των υπεύθυνων επεξεργασίας κατά τη στάθμιση είναι έτι δυσκολότερο[61]. Αφετέρου και μάλλον σημαντικότερα, το ζήτημα παρουσιάζει μια ενδιαφέρουσα ερμηνευτική υπόσταση, την αναλογικότητα των δικαιοδοτικών συστημάτων και την αξιολόγηση μεταξύ περισσότερων. Προφανώς η στάθμιση εκφεύγει των ορίων δύο κρατών και ανάγεται σε θέμα παγκόσμιας εμβέλειας. Η δυνητική πρόσβαση υποκειμένων δικαίου με κατοικία στην ΕΕ θέτει τον ΓΚΠΔ αυτομάτως εφαρμόσιμο. Η δε εφαρμογή του Κανονισμού ανοίγει αυτομάτως το ζήτημα της σύγκρισης και της στάθμισης των προστατευτικών πλαισίων.

Σε αυτό το σημείο, οι συμβατικές ρήτρες *Standard Contractual Clauses* (SCC), οι οποίες ήταν

[60] N. Härting, *Art. 23 Abs. 1 DS-GVO (Privacy by Design): Cupcake ohne Rezept*, Privacy in Germany, 5/2015, σελ. 193.
[61] Link, (τελευταία πρόσβαση 11.08.2022).

σε ισχύ κατά το παλαιό καθεστώς της προϊσχύσασας Οδηγίας 95/46 και επεκτάθηκαν και στο καθεστώς του ΓΚΠΔ, αποτελούν μια ενδεχόμενη λύση. Κατά τη δημιουργία του blockchain, οι χρήστες θα πρέπει να συμφωνήσουν και να αποδεχτούν το περιεχόμενο των πρότυπων ρητρών αυτών, ώστε να ενσωματωθεί ως ένα υποχρεωτικό πλαίσιο προστασίας στο blockchain, το οποίο θα ακολουθεί το επίπεδο προστασίας του ΓΚΠΔ[62]. Οι ρήτρες αυτές διευκολύνουν και επιτρέπουν τη διεθνή μεταφορά δεδομένων και εκτός ΕΕ, με την παράλληλη διασφάλιση εφαρμογής στα προς μεταφορά δεδομένα του προστατευτικού πλαισίου του ενωσιακού δικαίου, δηλαδή του ΓΚΠΔ.

VI. ΣΥΜΠΕΡΑΣΜΑΤΑ

Πρόθεση των Ευρωπαϊκών οργάνων μέσω της νομοθέτησης του Γενικού Κανονισμού για την Προστασία των Προσωπικών Δεδομένων αποτέλεσε η δημιουργία μίας αδιάτρητης ζώνης προστασίας των προσωπικών δεδομένων των πολιτών στην Ευρωπαϊκή Ένωση ενόψει των αυξανόμενων τεχνολογικών αναγκών με αυστηρούς και απαρέγκλιτους κανόνες. Για αυτό τον λόγο επιλέχθηκε ο ΓΚΠΔ να φέρει το εγγενές γνώρισμα της τεχνολογικής ουδετερότητας, γεγονός που του επιτρέπει μέσω της δυναμικής ερμηνείας των διατάξεων να προσαρμόζεται με χαμαιλεοντικό τρόπο στο τεχνολογικό περιβάλλον. Αντιλαμβανόμαστε, από τη μία, ότι ο Γενικός Κανονισμός, αντιπροσωπεύει ένα πατερναλιστικό/ προστατευτικό πρότυπο νομοθέτησης, το οποίο σκοπεί να ελέγξει όλες τις μορφές επεξεργασίας και να επιβάλλει αυξημένες υποχρεώσεις στις επιχειρήσεις με λιγοστά περιθώρια ευελιξίας.

Τα συστήματα blockchain, και η εποχή του Web 3.0, εισάγουν ένα νέο περιβάλλον με διακριτά χαρακτηριστικά από τα υπόλοιπα. Τούτο που επιχειρείται μέσω της τεχνολογίας είναι η δημιουργία δεσμών πίστης σε ένα λογισμικό με αυξημένες δυνατότητες και η ελαχιστοποίηση του παράγοντα της τυχαιότητας που επιτάσσουν οι σύγχρονες συναλλαγές. Οι αποτελεσματικότητες που διαγιγνώσκονται είναι πληθώρες και η πρακτική εφαρμογή έτι σημαντικότερη, η τελεολογία ωστόσο που λανθάνει αφορά στην αυτοματοποίηση και τη διευκόλυνση των άκαμπτων εν πολλοίς επιχειρησιακών μοντέλων με δημοκρατικοποίηση των άλλως ανισόρροπων διαδικασιών.

Η επιφυλακτική στάση των αρχών και των οργάνων καταρχήν δικαιολογείται εν όψει της αντίρροπης τελεολογίας των δύο συστημάτων και της αυξημένης ανάγκης διασφάλισης ενός *minimum* δικαιωμάτων. Πράγματι, η Ευρωπαϊκή Ένωση είναι ένας χώρος όπου τα πρόσωπα μπορούν να ορίζουν τις ροές δεδομένων που τα αφορούν, να ενημερώνονται κατάλληλα, να λησμονούνται και να αντιτίθενται νομικά σε κάθε παράνομη επεξεργασία σε βάρος τους. Ωστόσο, μια προστασία που ανταποκρίνεται σε παρωχημένα ή μόνο συγκεκριμένα συστήματα είναι ίσως πιο επικίνδυνη από την ανομία ή την έλλειψη νομοθέτησης διότι δύναται να εκμηδενίσει την καινοτόμο δράση. Σαφέστατα η τελευταία δεν μπορεί να στρέφεται κατά άλλων θεσμικών εγγυήσεων που συνιστούν σήμερα τα θεμέλια των ανθρώπινων ελευθεριών, όπως χαρακτηριστικά συνιστούν τα προσωπικά δεδομένα. Για αυτό τον λόγο, η εύρεση του σημείου χρυσής τομής στη στάθμιση μεταξύ ιδιωτικότητας και καινοτομίας απαιτεί ενισχυμένες, σύνθετες και τεχνικές δεξιότητες από τον ερμηνευτή, αλλά ενδεχομένως και άμεση νομοθετική καθοδήγηση με τη μορφή Κατευθυντηρίων Γραμμών σχετικά με την εφαρμογή των κανόνων του Γενικού Κανονισμού σε περιπτώσεις συστημάτων κατανεμημένου καθολικού, κατά τη συνήθη πρακτική του Ευρωπαϊκού Συμβουλίου Προστασίας

[62] Βλ. M. Artzt/L. Determann/W. Long, «Chapter 5: Blockchain and Data Privacy», ό.π., σελ. 242.

Δεδομένων (ΕΣΠΔ). Οι παραδεδεγμένες αρχές του δικαίου, όπως είναι λόγου χάριν η αρχή της αναλογικότητας ή η αρχή της νομιμότητας, σίγουρα εφαρμόζονται διαχρονικά και περιορίζουν αισθητά τα περιθώρια ελεύθερης ερμηνείας στο πεδίο των δικαιωμάτων. Ωστόσο, τα όρια μεταξύ ερμηνείας και de facto νομοθέτησης τείνουν στην πράξη να είναι ρευστά και με τη σειρά της η ερμηνευτική προσέγγιση εκ μέρους όλων των χωρών της ΕΕ οφείλει να είναι καθολική. ❑