ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΑ»

«ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΓΡΑΦΩΝ»

Του Μαυρέλου Ιωάννη (Α.Μ.: ΜΔΟ1636)

Επιβλέπουσα καθηγήτρια:

Δελούκα-Ιγγλέση Κορνηλία

ΠΕΙΡΑΙΑΣ, 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΑ»

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών του Πανεπιστημίου Πειραιώς «Δίκαιο και Οικονομία» με τίτλο «Νομικά Ζητήματα Ηλεκτρονικών Υπογραφών» έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου

Ο υπογράφων μεταπτυχιακός φοιτητής

Μαυρέλος Ιωάννης

Ημερομηνία: 22-06-2020

Ευχαριστίες

Η εκπόνηση της παρούσας δεν θα μπορούσε να έχει ολοκληρωθεί, χωρίς την αρωγή και την καθοδήγηση της επιβλέπουσας καθηγήτριας κας Δελούκα-Ιγγλέση Κορνηλίας, την οποία και θερμά ευχαριστώ.

Επιπλέον, και από το παρόν σημείο εκφράζονται οι ευχαριστίες μου προς την οικογένεια μου για την υποστήριξή τους καθ' όλη τη διάρκεια των μεταπτυχιακών σπουδών μου, και δη προς τον αδελφό μου για τις χρήσιμες επεξηγήσεις στα ζητήματα κρυπτογραφίας της παρούσης εργασίας. Ιδιαίτερη μνεία θα πρέπει να γίνει στην Παπαχριστοπούλου Ιωάννα-Ηλιάνα, η οποία αφειδώς μου παρείχε τη βοήθειά της κατά την εκπόνηση της εργασίας, στη Σπηλιοτοπούλου Χριστίνα, της οποίας η διάνοια και το ήθος έχω την τύχη να με συντροφεύουν επί σειρά ετών, και τέλος στο Δρ. Εφεντάκη Παναγιώτη, του οποίου η στάση και ο επαγγελματισμός αποτέλεσαν παράδειγμα προς μίμηση.

Περίληψη

Στην παρούσα διπλωματική εργασία προσεγγίζεται το θέμα των νομικών ζητημάτων που άπτονται των ηλεκτρονικών υπογραφών. Προκειμένου να γίνει αντιληπτή η σημασία τους στο ψηφιακό χώρο (και δη στις ιδιωτικές συναλλαγές) θα αναλυθεί η φύση και η λειτουργία τους υπό το πρίσμα των διατάξεων του νέου Κανονισμού (Ε.Ε.) αρ. 910/2014, αλλά και η στάση της ελληνικής νομολογίας απέναντι στα νομικά ζητήματα που ανακύπτουν.

Στο εισαγωγικό κεφάλαιο, δια της παρουσιάσεως της σημασίας των ηλεκτρονικών συναλλαγών και της ανάγκης ασφαλούς διεξαγωγής τους, αναδεικνύεται ο σημαντικός ρόλος των ηλεκτρονικών υπογραφών, οι οποίες συνιστούν προϋπόθεση, όχι μόνο κύρους των ηλεκτρονικών εγγράφων και της ηλεκτρονικής δικαιοπραξίας, αλλά σε μεγάλο βαθμό παρέχουν την πολυπόθητη ασφάλεια συναλλαγών. Στο δε πρώτο κεφάλαιο, γίνεται προσέγγιση των ηλεκτρονικών εγγράφων και της κατηγοριοποίησής τους, αφού αυτά αποτελούν στοιχείο αναπόσπαστο των ηλεκτρονικών συναλλαγών και φορέα της δήλωσης βουλήσεως των κοινωνών του διαδικτύου.

Στο δεύτερο κεφάλαιο, εξετάζεται το ζήτημα της νομικής φύσεως αλλά και της σημασίας της ηλεκτρονικής υπογραφής. Ειδικότερα, αφού εξεταστεί η ιδιόχειρη υπογραφή ως στοιχείου του κύρους ενός εγγράφου, επιχειρείται η προσέγγιση των ηλεκτρονικών υπογραφών. Εξετάζονται δε, όχι μόνο η μορφή που αυτή λαμβάνει και οι νομικοί ορισμοί που έχουν αποδοθεί σχετικά, αλλά επιχειρείται τελολογική προσέγγιση των τελευταίων.

Στο τρίτο κεφάλαιο επιχειρείται η προσέγγιση των ειδών-κατηγοριών των ηλεκτρονικών υπογραφών. Αρχικά, αναφορά γίνεται στα τρία βασικά είδη ηλεκτρονικών υπογραφών, τα οποία εξασφαλίζουν τη μεγαλύτερη δυνατή ασφάλεια στο χώρο του διαδικτύου με εκτενή ανάλυση των μεθόδων κρυπτογραφίας που χρησιμοποιούνται στις περιπτώσεις των ηλεκτρονικών υπογραφών. Στο ίδιο κεφάλαιο παρουσιάζεται η τριπλή διάκριση των ηλεκτρονικών υπογραφών, όπως αυτή τίθεται στον ισχύοντα πλέον Κανονισμό, καθώς και οι προβλέψεις του τελευταίου αναφορικά με τις εγκεκριμένες ηλεκτρονικές υπογραφές, τις εν γένει εγκεκριμένες ηλεκτρονικές υπογραφές .

Εν συνεχεία, στο τέταρτο κεφάλαιο, δεδομένου ότι η προσέγγιση του θέματος πραγματοποιείται υπό το πρίσμα του ισχύοντος νομοθετικού πλαισίου, επιχειρείται η παρουσίαση των κύριων νομοθετικών κειμένων που αφορούν τις ηλεκτρονικές υπογραφές. Ειδικότερα, εφαλτήριο θα αποτελέσει η επισκόπηση, τόσο της Οδηγίας 1999/93, όσο και του Π.Δ 150/2001 με το οποίο ενσωματώθηκε η τελευταία στην ελληνική έννομη τάξη. Ακολούθως, σχολιάζονται εκτενέστερα οι διατάξεις που αφορούν τις ηλεκτρονικές υπογραφές σύμφωνα με το νέο Κανονισμού (Ε.Ε.) αρ. 910/2014, ο οποίος ήδη από 01-07-2016 είναι εφαρμοστέος σε όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης, ενόσω, παράλληλα, καταργεί την Οδηγία 1999/93.

Στο έκτο κεφάλαιο, πραγματοποιείται μια σύντομη επισκόπηση της ελληνικής νομολογίας των Πολιτικών Δικαστηρίων. Σκοπός του κεφαλαίου είναι η ανάδειξη των νομικών ζητημάτων, τα οποία έχουν ανακύψει στην ελληνική έννομη τάξη και πως αυτά επιλύονται.

Τέλος, παρουσιάζονται τα συμπεράσματα που προκύπτουν από την παρούσα, ενώ δεν παραλείπεται να επισημανθεί η προτεινόμενη προσέγγιση των υφιστάμενων ρυθμίσεων από τον (ελληνικό) νομικό κόσμο.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΚ	Αστικός Κώδικας
ΑΠ	Άρειος Πάγος
αρ.	αριθμός
ΑΡΜ	Αρμενόπουλος (περιοδικό)
ΒΝΔ	Βάση Νομικών Δεδομένων
Δ	Δίκη (περιοδικό)
ΔΕΕ	Δίκαιο Επιχειρήσεων και Εταιριών (περιοδικό)
Δ/νη	Δικαιοσύνη
Επ.	επόμενα
ΕΕΤ	Ένωση Ελληνικών Τραπεζών
ΕΠολΔ	Επισκίπηση Πολιτικής Δικονομίας (περιοδικό)
Εφ.	Εφετείο
ΕφΑΔ	Εφαρμογές Αστικού Δικαίου (περιοδικό)
Η/Υ	Ηλεκτρονικός Υπολογιστής
ΚΔΔιαδ	Κώδικας Διοικητικής Διαδικασίας
ΚΠολΔ	Κώδικας Πολιτικής Δικονομίας
ΜονΠρ	Μονομελές Πρωτοδικείο
ΝοΒ	Νομικό Βήμα
παρ.	Παρ.
π.δ.	προεδρικό διάταγμα
ΠολΠρ	Πολυμελές Πρωτοδικείο
π.χ.	παραδείγματος χάριν
σ.	σελίδα
ΣΤΕ	Συμβούλιο της Επικρατείας

Εισαγωγή

Τις τελευταίες δεκαετίες έχουμε γίνει θεατές των αλμάτων της τεχνολογίας σε όλους τους τομείς και ειδικότερα αυτόν της πληροφορικής, η οποία έχει συμβάλει σε μία εκ βάθρων αλλαγή της καθημερινότητάς μας. Ενώ στην πρώτη βιομηχανική επανάσταση η ανθρωπότητα μηχανοποίησε την παραγωγή με την ατμομηχανή και κατά τη δεύτερη την μαζικοποίησε με την ηλεκτρική ενέργεια, στην τέταρτη εκμεταλλευόμαστε τα πλεονεκτήματα της αυτοματοποίησης της παραγωγής με τη χρήση των ηλεκτρονικών συστημάτων της τρίτης επαναστάσεως, ενώ πλέον, λόγω της ωριμότητας και άλλων τεχνολογιών[1] ενισχύονται οι ανωτέρω δυνατότητες με έξυπνα και αυτόνομα συστήματα τροφοδοτούμενα από σωρεία δεδομένων.[2]

Παρά τις ανωτέρω όμως αλλαγές, ήδη από την τρίτη βιομηχανική επανάσταση, με την ψηφιοποιήσει της παραγωγής, οι πολίτες-συναλλασσόμενοι είχαμε ήδη καταστεί συμμετέχοντες στην «Κοινωνία της Πληροφορίας», ήτοι «μία νέα μορφή κοινωνικής και οικονομικής ανάπτυξης, όπου οι τεχνολογίες της πληροφορικής και της επικοινωνίας έχουν κεντρική σημασία για την παραγωγή, την οικονομία αλλά και την κοινωνία γενικότερα».[3] Με

---

[1] «Η κυρίαρχη συζήτηση σήμερα, περιγράφει και προαναγγέλλει τη διαμόρφωση ενός νέου τεχνολογικού και αναπτυξιακού υποδείγματος, σε παγκόσμιο επίπεδο, το οποίο οδηγεί ταχύτατα σε μια ευρύτερη μετάβαση προς μια νέα «βιομηχανική εποχή» (την αποκαλούμενη «4η Βιομηχανική Επανάσταση») όπου βασική παράμετρος είναι, μεταξύ άλλων, η έννοια της «ψηφιοποίησης» και του ψηφιακού μετασχηματισμού των τομέων της οικονομίας, με ό, τι αυτά τα συνθέτουν (…) Ειδικότερα, η ανάδυση αυτού που σήμερα ονομάζουμε «4η Βιομηχανική Επανάσταση» χαρακτηρίζεται από ένα συνδυασμό τεχνολογικών συστημάτων που αναμιγνύουν τις σφαίρες του ενσώματου, του ψηφιακού και του βιολογικού κόσμου», βλ. Αντώνης Αγγελάκης (2019), «Η προαναγγελθείσα επανάσταση: τεχνολογική αλλαγή και προεκτάσεις υπό το πρίσμα της «4ης Βιομηχανικής Εποχής» Μέρος Ι - Θεωρητική επισκόπηση, Ερευνητικά Κείμενα ΙΜΕ ΓΣΕΒΕΕ, 6/2019, σ. 7-8, διαθέσιμο στην ιστοσελίδα https://imegsevee.gr/wp-content/uploads/2019/10/4%CE%B7-CE%B2%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%B5%CF%80%CE%B1%CE%BD%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7_%CE%BC1.pdf (ημερομηνία επίσκεψης: 28-05-2020). Για τις τεχνολογίες δε που αξιοποιούνται στα πλαίσια της 4ης Βιομηχανικής επανάστασης βλ. και Σταύρο Κουμεντάκη , «Η 4η Βιομηχανική Επανάσταση - Ρυθμίζεται, άραγε, η ανάπτυξη;», Capital.gr, 03-10-2019 διαθέσιμο στην ιστοσελίδα https://www.capital.gr/arthra/3385609/i-4i-biomixaniki-epanastasi-ruthmizetai-arage-i-anaptuxi (ημερομηνία επίσκεψης: 28-05-2020), όπου ενδεικτικά αναφέρονται:: Το Διαδίκτυο των πραγμάτων (Internet of Things -IoT), η ρομποτική (Robotics), η εικονική πραγματικότητα (Virtual Reality – VR), η τεχνολογία επαυξημένης πραγματικότητας (Augmented Reality), η Τεχνητή Νοημοσύνη (Artificial Intelligence-AI), ο ψηφιακός μετασχηματισμός (Digital transformation), η Τεχνολογία Κατανεμημένου Καθολικού (Distributed Ledger Technology - DLT), η Αλυσίδα Συστοιχιών (Blockchain), τα έξυπνα συμβόλαια (Smart Contract), Οικονομία Πλατφόρμων (Platform economy), η συμμετοχική (ή συνεργατική) οικονομία (Share/sharing economy),η ψηφιακή προσέγγιση της τεχνολογίας (Digital energy),η ψηφιακή υγεία (Digital health), τα συστήματα μη επανδρωμένων αεροσκαφών (Drones), καθώς και η τρισδιάστατη Εκτύπωση (3D Printing).

[2] Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation For Anyone", Forbes 02-09-2018, διαθέσιμο στην ηλεκτρονική διεύθυνση https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#1a5b52999788 (ημερομηνία επίσκεψης: 28-05-2020).

[3] Κορνηλία Δελούκα-Ιγγλέση, Νομικά Θέματα Ηλεκτρονικού Εμπορίου. 2η έκδ. Εκδόσεις Σακούλας, Αθήνα-Θεσσαλονίκη, σ. 1

την αυγή της νέας αυτής εποχής παρατηρείται η μεταφορά των συναλλαγών στο ηλεκτρονικό-ψηφιακό περιβάλλον. Μάλιστα, παρατηρείται ένας αμφίδρομος κύκλος, κατά τον οποίο οι συναλλασσόμενοι αξιοποιούν τα υπάρχοντα ηλεκτρονικά συστήματα – δίκτυα, ενώ με τη σειρά τους τα τελευταία εξελίσσονται, προκειμένου να εξυπηρετήσουν του πρώτους. Τα δίκτυα αυτά, άλλοτε χαρακτηρίζονται ως κλειστά και άλλοτε ανοιχτά με γνώμονα, την εκ των προτέρων άδειας πρόσβασης σε αυτά των χρηστών.[4] Ανοιχτό δίκτυο είναι το διαδίκτυο, το οποίο εξυπηρετεί το μεγαλύτερο αριθμό χρηστών υποστηρίζοντας συνεπώς και το μεγαλύτερο όγκο συναλλαγών ακριβώς λόγω της ανοιχτής δομής του.[5] Η ελεύθερη πρόσβαση σε αυτό καθιστά ευχερή, όχι μόνο την επικοινωνία μεταξύ των χρηστών σε παγκόσμια βάση, αλλά και τις συναλλαγές, επηρεάζοντας τις τόσο μεταξύ επιχειρήσεων (B2B), όσο και επιχειρήσεων με τους καταναλωτές (B2C), θέτοντας πλέον σε μία νέα βάση θεμελιώδη ζητήματα της αγοράς, όπως ο και ο ανταγωνισμός.[6]

Θα πρέπει να σημειωθεί ότι ο μεγάλος όγκος πληροφοριών που ανταλλάσσονται, καθώς και ο μαζικός αριθμός των διενεργούμενων συναλλαγών στο διαδίκτυο έχουν καταστήσει επιτακτική την ανάγκη διασφάλισης τους. Σε αντίθεση με τα εκ των προτέρων οριοθετημένα κλειστά δίκτυα, ο κίνδυνος είναι ιδιαίτερος στην περίπτωση του διαδικτύου, το οποίο αποτελεί ανοικτή βάση ελεύθερη σε όλους. Ο κίνδυνος δε που ενδέχεται να αντιμετωπίσει ο χρήστης κατά τις συναλλαγές του μπορεί να συνίσταται τόσο στην παρακολούθηση και υποκλοπή τόσο των δεδομένων που δέχεται/αποστέλλει, όσο και των προσωπικών απόρρητων κωδικών του καθιστώντας ευάλωτα εμπιστευτικά του στοιχεία. Δεδομένου δε ότι το διαδίκτυο αποτελεί ένα απρόσωπο μέσο επικοινωνίας ιδιαίτερα σημαντικός είναι και κίνδυνος της αλλοίωσης της

---

[4] Κωνσταντίνος Χριστοδούλου, (2000) «Τρία νέα ζητήματα του δικαίου των ηλεκτρονικών εγγράφων μετά το σχέδιο νόμου ηλεκτρονικές υπογραφές» Δ. 2000, σ. 1, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=&mnu=0&id=18351 (ημερομηνία επίσκεψης 10-05-2019)

Βλ. και Κ. Δελούκα-Ιγγλέση, ο.π. σ. 8-9. *«Με κριτήριο το χρησιμοποιούμενο δίκτυο το ηλεκτρονικό εμπόριο μπορεί να διακριθεί σε : α) Εκείνο που πραγματοποιείται μέσω ανοικτού δικτύου. Ανοικτό δίκτυο είναι αυτό στο οποίο μπορεί να έχει πρόσβαση οποιοσδήποτε διαθέτει τα απαραίτητα τεχνικά μέσα. Το γνωστότερο και πιο διαδεδομένο ανοικτό δίκτυο είναι το Διαδίκτυο, στο οποίο έχουν πρόσβαση Εκατομμύρια άνθρωποι σε όλη τη γη και μέσω του οποίου μπορούν να αναζητήσουν πληροφορίες, να προμηθευτούν προσόντα και υπηρεσίες, χρησιμοποιώντας το ως μέσο διαβίβασης δηλώσεων βούλησης για τη σύναψη συμβάσεων ή την κατάρτιση δικαιοπραξιών. β) Εκείνο που πραγματοποιείται μέσω κλειστού δικτύου. Κλειστό είναι το δίκτυο όταν σε αυτό συμμετέχουν ορισμένα μόνο πρόσωπα (π.χ. τραπεζικά ιδρύματα, επιχειρήσεις κ.λπ.) τα οποία έχουν αποδεχθεί εκ των προτέρων συγκεκριμένους κανόνες και διατυπώσεις ως προς τη διαβίβαση των δεδομένων, όπως είναι π.χ. το EDI (Electronic Data Interchange) που αποτελεί ένα εξελιγμένο σύστημα ηλεκτρονικής επικοινωνίας που συνίσταται σε μια μέθοδο τυποποίησης των δεδομένων».*

[5] Κωνσταντίνος Χριστοδούλου, ό.π. σ. 1., ομοίως σε Γ. Ζέκο, Διαδίκτυο, Η/Υ & τηλεπικοινωνίες στο ελληνικό δίκαιο, εκδόσεις Σάκκουλας Αθήνα-Θεσσαλονίκη, 2017, σ. 73

[6] Πέτρος Α. Καρέκλης Π (2003), Επιπτώσεις του Internet στη λειτουργία και κερδοφορία των επιχειρήσεων-Οφέλη από τη χρήση Υπηρεσιών ηλεκτρονικής τραπεζικής, Δελτίον Ένωσης Ελληνικών Τραπεζών Ιούλιος-Αύγουστος-Σεπτέμβριος 2003 σ. 41-44 διαθέσιμο στην ηλεκτρονική διεύθυνση https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/3_2003.pdf (ημερομηνία επίσκεψης 03-04-2020).

πληροφορίας που θέλει να μεταδώσει ο χρήστης. Δεδομένων τούτων γίνεται αντιληπτό ότι για την εμπέδωση της ασφάλειας των ηλεκτρονικών συναλλαγών θα πρέπει να συντρέχουν ορισμένες προϋποθέσεις, οι οποίες λειτουργούν ως δικλείδες ασφαλείας προς τους προαναφερθέντες κινδύνους.[7]

Ειδικότερα, θα πρέπει να καθίσταται εφικτή η αναγνώριση της αυθεντικότητας της ταυτότητας του κάθε χρήστη/συναλλασσόμενου (authentication), δεδομένου του υπέρογκου αριθμού άγνωστων μεταξύ τους συναλλασσόμενων. Ιδιαίτερης βαρύτητας κρίνεται και η δυνατότητα διαφύλαξης της ακεραιότητας του περιεχομένου μηνύματος (integrity) από τυχόν απόπειρες αλλοίωσης του παραλαμβανόμενου μηνύματος. Συναφώς, λόγω (και) των απρόσωπων σχέσεων, θα πρέπει να εξασφαλίζεται ότι ο αποστολέας του μηνύματος δεν θα μπορεί να αποποιηθεί εκ των υστέρων το περιεχόμενο του μηνύματος που απέστειλε (non-repudation). Τέλος, προκειμένου να μην μπορέσει κάποιος τρίτος να λάβει γνώση του περιεχομένου του μηνύματος, παρά τη θέληση των μερών, θα πρέπει να διασφαλίζεται η εμπιστευτικότητα (confidentiality).[8]

Μάλιστα, το πλέον διαδεδομένο μηχανικό μέσο για τη διακίνηση πληροφοριών, αλλά και την διενέργεια συναλλαγών στο διαδίκτυο είναι τα λεγόμενα ηλεκτρονικά έγγραφα. Ενόψει όμως των κινδύνων του διαδικτύου, άρα και των συνακόλουθων απαιτήσεων ασφαλούς επικοινωνίας και ασφαλών συναλλαγών, δημιουργείται εύλογα το ερώτημα, πως μπορεί ο χρήστης του διαδικτύου να θωρακιστεί. Επιπροσθέτως, τίθεται επιτακτικό το ερώτημα, πως μπορεί να διασφαλιστεί η εγκυρότητα των ηλεκτρονικών δικαιοπραξιών, όταν σε αυτές απαιτείται έγγραφος τύπος. Οι ανωτέρω ανάγκες ασφαλούς επικοινωνίας, αλλά κυρίως ασφαλών συναλλαγών καλύπτονται δια των ηλεκτρονικών υπογραφών και δη στον (κατά το δυνατό) μέγιστο βαθμό δια των προηγμένων[9] και δη σε ό, τι αφορά το τελευταίο ερώτημα των εγκεκριμένων ηλεκτρονικών υπογραφών ως κατωτέρω θα αναλυθεί στην παρούσα εργασία.[10] Αντιλαμβάνεται κανείς ότι στο νέο αυτό περιβάλλον ο νομοθέτης (εθνικός και ενωσιακός) καλείται να διαδραματίσει καίριο ρόλο, αφού από τη μία θα πρέπει να παρέχει ένα επαρκές δικαιϊκό πλαίσιο, το οποίο θα εξασφαλίζει την πολυπόθητη ασφάλεια δικαίου, ενώ ταυτόχρονα

---

[7] Κοσμάς Καραδημητρίου, Η Ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο, Μη Εκδοθείσα Διδακτορική Διατριβή. Αριστοτέλειο Πανεπιστήμιο, 2007, σ. 43-46,
Χρυσούλα Μιχαηλίδου, Το πρόβλημα της ηλεκτρονικής υπογραφής. Δ. 2000, σ. 1-2 διαθέσιμο στην ηλεκτροτεχνική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=1479&mnu=3&id=18381 (ημερομηνία επίσκεψης 16-03-2020]
Κωνσταντίνος Χριστοδούλου υπ., σ. 3

[8] Κωνσταντίνος Χριστοδούλου ό.π., σ. 3. Ομοίως Καραδημητρίου όπ. σσ. 47-48

[9] Κοσμάς Χριστοδούλου, ό.π., σελ. 48.

[10] Χρυσούλα Μιχαηλίδου, ό.π. σ. 3 Το πρόβλημα της ηλεκτρονικής υπογραφής. Δ. 2000, σ. διαθέσιμο στην ηλεκτροτεχνική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=1479&mnu=3&id=18381 (ημερομηνία επίσκεψης 16-03-2020]

δεν θα πρέπει να σταθεί εμπόδιο στις τεχνολογικές εξελίξεις, ούτε βέβαια να τις ακολουθεί από απόσταση.[11]

Με την παρούσα διπλωματική εργασία επιχειρείται να εξετασθούν τα νομικά ζητήματα, τα οποία αφορούν τις ηλεκτρονικές υπογραφές. Αρχικά, προσεγγίζεται η έννοια των ηλεκτρονικών εγγράφων, ήτοι των μέσων που αξιοποιούνται στο ψηφιακό περιβάλλον για τη μεταβίβαση ενός μηνύματος. Εν συνεχεία εξετάζεται η φύση των ηλεκτρονικών υπογραφών και οι λειτουργίες που αυτές επιτελούν.

Η Ε.Ε. στην προσπάθεια οικοδόμησης εμπιστοσύνης στο ψηφιακό περιβάλλον και στην κατεύθυνση της ολοκλήρωσης της ψηφιακής ενιαίας αγοράς, εξέδωσε τον Κανονισμό (Ε.Ε.) 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/Ε.Ε..[12] Επιχειρείται δε η περιγραφή των μεθόδων που αξιοποιούνται για τη δημιουργία ηλεκτρονικών υπογραφών, ενώ έμφαση δίνεται στις κατηγορίες και στις προϋποθέσεις που απαιτεί ο ισχύον Κανονισμός (Ε.Ε.) 910/2014 για τις ηλεκτρονικές υπογραφές[13], ο οποίος κατήργησε την παλαιότερη Οδηγία 99/93/ΕΚ αντικαθιστώντας έτσι στο εθνικό δίκαιο τις διατάξεις, οι οποίες αναφέρονταν σε αυτήν (την Οδηγία). Πράγματι, όπως φάνηκε στην πράξη, η επιλογή εκ μέρους του Κοινοτικού νομοθέτη μιας «Οδηγίας» αντί ενός «Κανονισμού» παρουσίασε σοβαρά προβλήματα όσον αφορά την εφαρμογή της στην πράξη καθώς κάθε κράτος-μέλος όριζε αυστηρότερες ή ηπιότερες προϋποθέσεις ως προς τις ηλεκτρονικές υπογραφές «κατά το δοκούν». Πέραν τούτου, όπως διαπιστώθηκε, και αυτό είναι και το σημαντικότερο, κανένα από τα κράτη-μέλη δεν είχε υιοθετήσει τα ίδια τεχνικά πρότυπα για την εφαρμογή των ηλεκτρονικών υπογραφών, αποτρέποντας έτσι μια πραγματική διαλειτουργικότητα.[14] Έτσι, όπως ρητά αναφέρεται στη δεύτερη αιτιολογική σκέψη του προοιμίου του Κανονισμού, επιδίωξη αυτού αποτελεί η ενίσχυση της εμπιστοσύνης στις

[11] Ι. Ιγγλεζάκης, Δίκαιο πληροφορικής, 3η έκδ., Εκδόσεις Αθήνα-Θεσσαλονίκη 2018, σ. 3

[12] Σύμφωνα με τη σκέψη 1 του προοιμίου του Κανονισμού (ΕΕ) 910/2014: *«Η οικοδόμηση εμπιστοσύνης στο επιγραμμικό περιβάλλον είναι καθοριστικής σημασίας για την οικονομική και κοινωνική ανάπτυξη. Η έλλειψη εμπιστοσύνης, ιδίως λόγω της φαινόμενης έλλειψης ασφάλειας δικαίου, κάνει τους καταναλωτές, τις επιχειρήσεις και τις δημόσιες αρχές να διστάζουν να πραγματοποιούν συναλλαγές ηλεκτρονικά και να υιοθετήσουν νέες υπηρεσίες».*

[13] Κανονισμός (Ε.Ε) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/Ε.Κ., ΕΕ L 257 της 28.8.2014.

[14] Βλ. και ανακοίνωση της Επιτροπής της 26ης Αυγούστου 2010 με τίτλο «Ψηφιακό θεματολόγιο για την Ευρώπη» διαθέσιμο στην ηλεκτρονική διεύθυνση https://ec.europa.eu/commission/presscorner/detail/el/MEMO_10_200 (ημερομηνία επίσκεψης 23-05-2020) «Η Ευρώπη εξακολουθεί να αποτελεί ένα συνονθύλευμα εθνικών επιγραμμικών αγορών, ενώ οι Ευρωπαίοι δεν μπορούν να απολαύσουν τα πλεονεκτήματα της ψηφιακής ενιαίας αγοράς. Το εμπορικό και το πολιτιστικό περιεχόμενο και οι υπηρεσίες πρέπει να κυκλοφορούν Εκατέρωθεν των συνόρων· τούτο πρέπει να επιτευχθεί με εξάλειψη των ρυθμιστικών φραγμών (…)»

ηλεκτρονικές συναλλαγές, εντός της εσωτερικής αγοράς[15]. Περαιτέρω, είναι σημαντικό να τονισθεί εξαρχής ότι, ο Κανονισμός (Ε.Ε.) 910/2014, επεμβαίνει στα εθνικά δικονομικά δίκαια καθώς εισάγει συγκεκριμένες «άμεσης εφαρμογής» διατάξεις για την αποδεικτική αξία συγκεκριμένων ηλεκτρονικών δεδομένων. Από την άλλη μεριά,, σε επίπεδο ουσιαστικού δικαίου, ο Κανονισμός, *«δεν θίγει το εθνικό ή ενωσιακό δίκαιο σε ό,τι αφορά τη σύναψη και την ισχύ συμβάσεων ή άλλων νομικών ή διαδικαστικών υποχρεώσεων ως προς τον τύπο»* (βλ. άρθρο 2 παρ. 3)[16].

Δεδομένου δε ότι θέσεις της θεωρίας και της νομολογίας για τις ηλεκτρονικές υπογραφές στηρίχτηκαν στο προϊσχύσαν δίκαιο, πραγματοποιείται μία κριτική επισκόπηση της Οδηγία 99/93/Ε.Κ. και του π.δ. 150/2001, καθώς και του Κανονισμού (Ε.Ε.) 910/2014 ως ισχύει σήμερα αναδεικνύοντας τα πλεονεκτήματά του. Επιπλέον, επιχειρείται η εξαγωγή συμπερασμάτων αναφορικά με τη στάση των ελληνικών πολιτικών δικαστηρίων ως προς τις ηλεκτρονικές υπογραφές. Τέλος, εξάγονται συμπεράσματα από το σύνολο της παρούσας έρευνα.

[15] Ειδικότερα, σύμφωνα με το σημείο 2 του προοιμίου του Κανονισμού: *«Επιδίωξη του κανονισμού είναι να ενισχυθεί η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές εντός της εσωτερικής αγοράς, με την παροχή κοινής βάσης για ασφαλείς ηλεκτρονικές αλληλεπιδράσεις μεταξύ των πολιτών, των επιχειρήσεων και των δημόσιων αρχών, αυξάνοντας έτσι την αποτελεσματικότητα των δημόσιων και ιδιωτικών επιγραμμικών υπηρεσιών, του ηλεκτρονικού επιχειρείν και του ηλεκτρονικού εμπορίου στην Ένωση».*

[16] Κομνηνός Κόμνιος, Το νέο ευρωπαϊκό νομοθετικό πλαίσιο για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης - Συναφή ζητήματα δικαίου απόδειξης, Εφαρμογές Αστικού Δικαίου & Πολιτικής Δικονομίας 6 (2017), σ. 498-510., σ. 498-499.

Κεφάλαιο 1ο: Τα ηλεκτρονικά έγγραφα

Στο παρόν κεφάλαιο παρουσιάζονται συνοπτικά τα ηλεκτρονικά έγγραφα, όχι μόνο λόγω της σημασίας τους κατά την αξιοποίηση των δυνατοτήτων του διαδικτύου, αλλά ως έννοια απαραίτητη για την κατανόηση των ηλεκτρονικών υπογραφών. Άλλωστε, τα ηλεκτρονικά έγγραφα αποτελούν τη ραχοκοκαλιά των ηλεκτρονικών συναλλαγών και της κοινωνίας της πληροφορίας γενικότερα. Πράγματι, τα ηλεκτρονικά έγγραφα κυριαρχούν στο χώρο του διαδικτύου, εάν λάβει κανείς υπ' όψιν του ότι ως ηλεκτρονικό έγγραφο νοείται κάθε είδους εγγραφή στην οθόνη του Η/Υ, όπως τα e-mails, οι ιστοσελίδες, τα αρχεία που διακινούνται μέσω του διαδικτύου, οι τηλεδιασκέψεις, κ.ο.κ.

Έτσι, πέραν των στοιχείων που τα διαφοροποιούν από τα πα ιδιαίτερων χαρακτηριστικών τους, εξετάζεται ο νομικός τους ορισμός, ενώ, για την πληρότητα της προσέγγισης, αναφορά γίνεται και στις ειδικότερες κατηγορίες αυτών.

1.1. Η έννοια των ηλεκτρονικών εγγράφων .

Στον ψηφιακό μάλιστα χώρο του διαδικτύου η δήλωση βουλήσεως οποιουδήποτε προσώπου διαβιβάζεται με ηλεκτρονικά μέσα, όπως ο ηλεκτρονικός υπολογιστής, ή το ηλεκτρονικό ταχυδρομείο.[17] Η διακίνηση εγγράφων και οι πληροφορίες που αυτά ενσωματώνουν αποτελούν αναπόσπαστο κομμάτι των δραστηριοτήτων και των συναλλαγών μεταξύ των χρηστών του διαδικτύου για τη διαβίβαση πληροφοριών, είτε αυτά αφορούν το εμπόριο, είτε απλά την ενημέρωση, είτε απλά διοικητικές διαδικασίες. Μάλιστα, οι περιεχόμενες σε αυτά πληροφορίες μπορεί να αποτυπώνουν στοιχεία ή και να αναπαράγουν πληροφορίες ακόμα και τηλεδιασκέψεων ή μαγνητοφωνημένων ομιλιών αποτυπωμένες σε αποθηκευτικά εργαλεία, όπως δισκέτες ή (περιφερειακοί) μαγνητικοί δίσκοι.[18] Θα πρέπει να σημειωθεί δε, ότι αυτά δεν είναι από μόνο του αναγνωρίσιμα, αλλά απαιτείται η μεσολάβηση της κατάλληλης τεχνολογίας (τεχνικής διαδικασίας), δηλαδή της μετατροπής των αρχειοθετημένων ηλεκτρονικών εγγραφών σε εικόνες, γράμματα και λέξεις.[19] Ακόμα, όμως κι έτσι αυτά απεικονίζουν μόνον ένα αφηρημένο νόημα, αφού σε αυτά περιέχονται μόνον νοητικά τους σύμβολα, λόγοι περί αυτών. Και τούτο διότι, η περιεχόμενη πληροφορία δεν έγκειται στο αισθητό αποτύπωμά του, αλλά απλώς στα περιεχόμενα νοητικά σύμβολα, όπως λέξεις προτάσεις αριθμούς, που μάλιστα δεν αντιστοιχούν κατ' ανάγκη σε γεγονότα, αλλά σε αφηρημένες έννοιες. Σε κάθε περίπτωση πάντως, ανεξαρτήτως του εάν η πληροφορία είναι αναγνωρίσιμη ή όχι, «από τη στιγμή που το

[17] Παπαθωμά Μπέτγκε Α., (1999) «Ηλεκτρονικό εμπόριο: Νομικά ζητήματα κατά τη σύναψη εμπορικών συμβάσεων στο Ίντερνετ», ΔΕΕ 12/1999,σ. 1238-1239

[18] Κωνστνατίνος Χριστοδούλου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία μετά τις νέες κοινοτικές ρυθμίσεις . 2η έκδοση. Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας 2004 , σ. 2-4

[19] Βλ. Κ. Δελούκα-Ιγγλέση, ό.π., σ. 178 επ.

νοηματικό περιεχόμενο του ηλεκτρονικού εγγράφου έχει αποθηκευθεί από την προσωρινή στη μόνιμη μνήμη του, θα πρέπει να γίνει δεκτό, ότι η σχετική δήλωση αποτυπώθηκε σ' αυτό.»[20]

Τα ηλεκτρονικά έγγραφα αποτελούν πράγμα κατά την 947 ΑΚ.[21] Όπως όμως έχει διαπιστωθεί[22] «τα συνήθη ιδιωτικά έγγραφα χρησιμοποιούν προς τούτο την γραφήν, ενώ αι μηχανικαί απεικονίσεις την οπτικήν ή ακουστικήν αποτύπωσιν - ακόμα και όταν το απεικονιζόμενον συνίσταται εις παράστασιν διά γραμμάτων» Ήδη από τα διδάγματα τη κοινής πείρας όμως, καθίσταται πασίδηλο ότι το ηλεκτρονικό έγγραφο διαφέρει ως προς τα στοιχεία του από την περιγραφή που μόλις παρατέθηκε. Και τούτο διότι από την ίδια τη φύση του αυτό δεν ενσωματώνεται – το περιεχόμενο του δηλαδή δεν καταχωρείται – σε ορισμένο υλικό φορέα. [23] Επιπλέον, το ηλεκτρονικό έγγραφο διαφοροποιείται και νομικά από τα έγγραφα του άρθρου 160 ΑΚ, διότι, πέραν της θέσης που επικρατεί περί μη σταθερής ενσωμάτωσης, δεν είναι εφικτό να φέρει ιδιόχειρη υπογραφή.[24]

Οι διαφοροποιήσεις αυτές καθιστούν απαιτητή την εξεύρεση ενός αποδεκτού ορισμού του ηλεκτρονικού εγγράφου. Έτσι, ως τέτοιο κατά έχει κριθεί ότι είναι *«το σύνολο των εγγραφών δεδομένων στον μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή, οι οποίες, αφού γίνουν αντικείμενο επεξεργασίας από την κεντρική μονάδα επεξεργασίας, αποτυπώνονται με βάση τις εντολές του προγράμματος κατά τρόπο αναγνώσιμο από τον άνθρωπο είτε στην οθόνη του μηχανήματος είτε στον προσαρτημένο εκτυπωτή του»* [25], άποψη την οποία με ελάχιστες κάθε

[20] Κωνστνατίνος Χριστοδούλου, ό.π., σ. 4-5, 6

[21] Κωνστνατίνος Χριστοδούλου, ό.π., σ. 5-6, όπου χαρακτηριστικά αναφέρει: «το ηλεκτρονικό έγγραφο είναι πράγμα, τόσο κατά τη διαβίβασή του, όσο και μετά τη λήψη του. Στην πρώτη περίπτωση με την έννοια της δεύτερης παραγράφου της ΑΚ 947, ήτοι της φυσικής και ειδικότερα της ηλεκτρομαγνητικής ενέργειας που υπόκειται σε εξουσιάσω και περιορισμό σε ορισμένο χώρο, δηλ. στα καλώδια και τελικά στον ηλεκτρονικό υπολογιστή. Στη δεύτερη περίπτωση, όταν δηλ. πια το ηλεκτρονικό μήνυμα έχει ληφθεί, εντυπωνόμενο στο δίσκο του υπολογιστή ή σε κάποια δισκέτα, α ή cd, τότε πια αυτά τα τελευταία αποτελούν το ηλεκτρονικό έγγραφο, όντας ο υλικός του φορέας. Στην περίπτωση αυτή το ηλεκτρονικό έγγραφο είναι πράγμα κατά την συνήθη έννοια του όρου, αυτήν της πρώτης παραγράφου της ΑΚ 947. Παραπέρα πρόβλημα δε νομίζω ότι αποτελεί το αν το ηλεκτρονικό έγγραφο συνιστά αυτοτελές πράγμα δεκτικό αυτοτελούς εξουσιάσου (..)»

[22] Μητσόπουλου Γ./Κεραμέως Κ., Το τηλετύπημα (TELEX) αποτελεί αρχή εγγράφου αποδείξεως υπέρ του αποστολέα του, NoB 31 (1983), σελ. 330-331

[23] Αμφιβολίες Εκφράζει Κωνστνατίνος Χριστοδούλου (ό.π., σ.6) κατά πόσον η ενσωμάτωση της δήλωσης στο ηλεκτρονικό έγγραφο είναι η μόνιμη αποτύπωση που αξιώνει ο νόμος προκειμένου για το ιδιωτικό έγγραφο, δεδομένης της δυνατότητας της μη αναγνωρίσιμης εκ των υστέρων αλλοίωσης του περιεχομένου του ηλεκτρονικού εγγράφου, εφόσον δεν υπάρχει έγχαρτη αποτύπωση του περιεχομένου του ηλεκτρονικού εγγράφου.
Πρβλ Δ. Μανιώτη, Η ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο. Αθήνα-Κομοτηνή: Αντ. Σάκκουλα1999,σ. 60, που υποστηρίζει ότι από τη στιγμή που τα ηλεκτρονικά έγγραφα αποθηκεύονται σε σταθερό μέσο (π.χ.: σε κάποιο μαγνητικό δίσκο), καθίσταται δυνατή η σταθερή και μόνιμη καταγραφή του περιεχομένου κατά τρόπο ανάλογο με αυτή των παραδοσιακών εγγράφων.

[24] Κοσμάς Α. Καραδημητρίου, ό.π., σ.33-34, Κωνστνατίνος Χριστοδούλου, ό.π., σ. 5-6,

[25] ΕφΑθ 46/2014 ΔΕΕ 4/2014 σ. 373, ΕφΑθ 32/2011 ΔΕΕ 5/2011 σ. 591, ΜονΠρΑθ 1963/2004, ΔιΜΕΕ 3/2004. = Δ. Μάιος 2005 με παρατηρήσεις Μπέη Κ., (2005), διαθέσιμο στην ηλεκτρονική διεύθυνση

φορά διαφοροποιήσεις δέχεται στη πλειοψηφία της η ελληνική νομολογία και μέρος της ελληνικής νομικής θεωρίας.[26]

Η ανωτέρω όμως προσέγγιση, καίτοι μπορεί να θεωρηθεί αρκετά κατατοπιστική, εν τοις πράγμασι μάλλον καταλήγει άσκοπα περιοριστική. Ειδικότερα, προκειμένου να θεωρηθεί ένα έγγραφο ως ηλεκτρονικό, θα πρέπει ο υλικός φορέας αποτυπώσεως να είναι μαγνητικός δίσκος.[27] Ωστόσο, οι τεχνολογικές εξελίξεις έχουν καταστήσει τη χρήση μαγνητικών δίσκων μάλλον παρωχημένη, αφού για σειρά ετών διαδεδομένη ήταν η χρήση οπτικών δίσκων (CDs/DVDs), ενώ πλέον όλο και πιο συχνή είναι η χρήση των λεγόμενων υπολογιστικών νεφών (computing clouds) από τους τελικούς χρήστες του διαδικτύου. Στην καθημερινή πρακτική θα ήταν αδιανόητο να περιορίσουμε τον ορισμό των ηλεκτρονικών εγγράφων αποκλειστικά σε εκείνα, τα οποία είναι «αναγνωρίσιμα από τον άνθρωπο» σε κάποια οθόνη ή μόνο δια της εκτυπώσεως. Μία τέτοια προσέγγιση δεν θα κάλυπτε ούτε τις μονομερώς απευθυντέες δηλώσεις, τις οποίες για οποιοδήποτε λόγο δεν θα «άνοιγε» ο παραλήπτης, αφού δεν θα εκτυπώνονταν ή θα εμφανίζονταν σε κάποια οθόνη, ούτε πληροφορίες, οι οποίες είναι κωδικοποιημένες σε μορφές αλγορίθμου μη αναγνωρίσιμες από κάποιο φυσικό πρόσωπο.[28] Συνεπώς, μία τυπολατρική προσκόλληση στον ανωτέρω ορισμό θα παρέβλεπε τα υπάρχοντα μέσα, αλλά και την πρακτική αξία (έστω και της μονομερούς) μετάδοσης της πληροφορίας.

Στον ανωτέρω (εν πολλοίς) περιγραφικό και περιοριστικό ορισμό αντιτάσσεται μέρος της θεωρίας[29] προτείνοντας μία ευρύτερη θεώρηση. Ειδικότερα, προτάθηκε ως ηλεκτρονικό έγγραφο να θεωρείται *«κάθε έγγραφο του οποίου η υπογραφή παράγεται (εξ ολοκλήρου ή απλώς αποτυπώνεται) με τη βοήθεια της ηλεκτρονικής τεχνολογίας»*. Στα πεδίο αυτού του ορισμού μπορεί να υπαχθεί οποιοδήποτε έγγραφο το οποίο παράχθηκε με τα σύγχρονα τεχνολογικά μέσα, ανεξαρτήτως εάν αυτά έχουν υλική υπόσταση ή αποτυπώνονται μόνο σε ηλεκτρονική

---

http://www.kostasbeys.gr/articles.php?s=5&mid=&mnu=0&id=21305&keyw=%CC%D0%F1%C1%E8+1963%2F2004&sr=search&pg= (ημερομηνία επίσκεψης 20-05-2019], ΜονΠρΑθ 1327/2001, ΔΕΕ 4/2001 με παρατηρήσεις Κοσούλη σ. 377 = Δ 32 (2001) με παρατηρήσεις Μπέη Κ., βλ. και ορισμό σε Χ.Μιχαηλίδου, ό.π., σελ. 3, ο οποίος μολονότι επικρίθηκε ως περιοριστικός ακολουθείτε από τη νομολογία ως σήμερα, όπως για παράδειγμα η υπ' αρ. 1085/2018 ΜονΠρΗρακλείου (ΒΝΔ NOMOS)

[26] Καράκωστας Γ., Δίκαιο και Internet: νομικά ζητήματα του διαδικτύου. 2η έκδοση. Αθήνα, Π.Ν. Σάκκουλας Θεσσαλονίκης 2003, σ. 191

Κοσούλης Σ, σε παρατηρήσεις επί της 1327/2001 ΜονΠρΑθηνών, ΔΕΕ 4/2001 σ. 377.

[27] Υπουργείο Εθνικής Παιδείας και Θρησκευμάτων – Παιδαγωγικό Ινστιτούτο (1999) «Τεχνολογία Υπολογιστικών Συστημάτων & Λειτουργικά Συστήματα», Αθήνα, Οργανισμός Εκδόσεως Διδακτικών Βιβλίων, μέρος 5, Διαθέσιμο στην ηλεκτρονική διεύθυνση http://ebooks.edu.gr/modules/ebook/show.php/DSB103/173/1204,4404/ (ημερομηνία τελευταίας επίσκεψης 18-01-2018.

[28] Κωνσταντίνος Χριστοδούλου Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία. Αθήνα-Κομοτηνή, Αντ. Ν Σακκουλας 2001, σ. 2-4

[29] Κωνσταντίνος Χριστοδούλου (2001), υπ., 4

μορφή. Μάλιστα, όπως υποστηρίζεται[30]ο ανωτέρω ορισμός ερείδεται κατά τρόπο έμμεσο στο άρθρο 2 του π.δ 150/2001, ήτοι το νόμο που εισήγαγε στην ελληνική έννομη τάξη την Οδηγία 1999/94 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου (με ταυτόλογη διάταξη στο άρθρο 2 παρ. 1 της Οδηγίας). Ειδικότερα, στον ορισμό της ηλεκτρονικής υπογραφής αναφέρεται ότι πρόκειται για *«δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας»*. Η ηλεκτρονική υπογραφή, δηλαδή, αξιοποιείται για την απόδειξη γνησιότητας ηλεκτρονικής μορφής δεδομένων, καθιστώντας αδιάφορη τόσο την εμφάνιση των εγγράφων σε κάποια οθόνη, όσο και το είδος του υλικού φορέα ενσωμάτωσης, όπως για παράδειγμα σε κάποιο σκληρό δίσκο, σε μαγνητική δισκέτα, σε CD ή σε υπολογιστικό νέφος.

Ωστόσο, με τη θέση σε ισχύ του Κανονισμού 910/2014 η ανωτέρω διάσταση απόψεων έλαβε τέλος, επιβεβαιώνοντας εκείνους που τάσσονταν υπέρ ενός ευρύτερου ορισμού. Ειδικότερα, στο άρθρο 3 στοιχ. 35, ως ηλεκτρονικό έγγραφο ορίζεται: *«οποιοδήποτε περιεχόμενο έχει αποθηκευτεί σε ηλεκτρονική μορφή και ειδικότερα ως κείμενο ή με ηχητική, οπτική ή οπτικοακουστική εγγραφή»*. Ο ίδιος ο ενωσιακός νομοθέτης δηλαδή υιοθετεί την πλέον ευρεία προσέγγιση των ηλεκτρονικών εγγράφων, αποσυνδέοντας δε τον τρόπο δημιουργίας-αποθήκευσης και την νομική τους υπόσταση τους από την ανάγκη αυτά να φέρουν ηλεκτρονική υπογραφή ή οποιοδήποτε άλλο αποδεικτικό γνησιότητάς τους[31]. Αναφορικά δε με τη μορφή (format) που μπορούν να λάβουν τα έγγραφα, η απαρίθμηση είναι σκοπίμως ενδεικτική, αφού δεν επιδιώκει τον περιορισμό των μέσων που μπορούν να χρησιμοποιηθούν. Θα πρέπει να σημειωθεί βέβαια ότι τα ελληνικά δικαστήρια μέχρι και σήμερα αξιοποιούν τον πρώτο ορισμό που δόθηκε,[32] παρά το γεγονός ότι πρόκειται για έναν ορισμό, αρκετά περιοριστικό. Σε κάθε περίπτωση όμως, δεδομένης της ισχύος του Κανονισμού (Ε.Ε.) αρ. 910/2014 θα πρέπει ως ηλεκτρονικό έγγραφο να γίνεται αντιληπτό οποιοδήποτε σύνολο δεδομένων, το οποίο αποδίδει ένα περιεχόμενο (πληροφοριών), ανεξαρτήτως του φορέα και της μορφής αποθήκευσης του (αφού άλλωστε χρησιμοποιεί ενδεικτική παράθεση μορφών αποθήκευσης).

1.2. Διακρίσεις των ηλεκτρονικών εγγράφων

[30] Κοσμάς Α. Καραδημητρίου, υπ., σ. 35

[31]« Κατ ουσίαν, ο ορισμός του ηλεκτρονικού εγγράφου σύμφωνα με το άρθρο 3 σημ. 35 του Κανονισμού προσιδιάζει στο εννοιολογικό περιεχόμενο των μηχανικών απεικονίσεων του άρθρου 444 παρ. 1γ και παρ. 2 ΚΠολ, αφού, ενώ τα ιδιωτικά έγγραφα του ΚΠολΔ χρησιμοποιούν τη γραφή ως μέθοδο ενσωμάτωσης και μετάδοσης του περιεχόμενου μηνύματος, οι μηχανικές απεικονίσεις χρησιμοποιούν «την οπτικήν ή ακουστικήν αποτύπωσιν – ακόμα και όταν το απεικονιζόμενο συνίσταται εις παράστασιν διά γραμμάτων», Έτσι, Κ. Κόμνιος, «Το νέο ευρωπαϊκό νομοθετικό πλαίσιο για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης - Συναφή ζητήματα δικαίου απόδειξης», ΕφΑΔ/2017, σ. 498.

[32] Βλ. και ανωτέρω υποσημείωση 22

Στα ηλεκτρονικά έγγραφα, όπως αυτά αναφέρθηκαν αμέσως ανωτέρω, ανάλογα με τη φορέα αποτύπωσής τους, αλλά και τις ισχύουσες νομικές ρυθμίσεις παρατηρούνται επιμέρους διακρίσεις.

Η πρώτη διάκριση εδράζεται στην υπόσταση που αυτά έχουν. Ειδικότερα, υπάρχουν οι περιπτώσεις των εγγράφων, τα οποία μπορεί να έχουν υλική μεν υπόσταση, αλλά το περιεχόμενο και η υπογραφή τους δημιουργήθηκαν ηλεκτρονικά. Στην περίπτωση αυτή κάνουμε λόγο για μη γνήσια ηλεκτρονικά έγγραφα, με πιο άμεσο παράδειγμα αυτό της τηλεομοιοτυπίας (Fax). Κατ' αντιπαραβολή, γίνεται αντιληπτό ότι τα γνήσια ηλεκτρονικά έγγραφα, αφορούν αυτές τις περιπτώσεις εγγράφων «έχουν αποκλειστικά ηλεκτρονική υπόσταση, δηλαδή καταχωρίσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό».[33] Βέβαια, σε ό,τι αφορά την τελευταία περίπτωση, εν όψει του ορισμού του ισχύοντος Κανονισμού για τα ηλεκτρονικά έγγραφα αλλά και των προσεγγίσεων που ήδη εκτέθηκαν, συνετό θα ήταν να επιχειρηθεί διασταλτική ερμηνεία του ορισμού των γνήσιων ηλεκτρονικών εγγράφων, ώστε να περιλαμβάνονται άπαντα με ηλεκτρονική υπόσταση, ανεξαρτήτως αποθηκευτικού μέσου.[34]

Η δεύτερη διάκριση που αφορά στα ηλεκτρονικά έγγραφα έγκειται στο κατά πόσο πληρούν τις προϋποθέσεις του (εκάστοτε ισχύοντος) θεσμικού πλαισίου, ώστε αυτά να εξομοιώνονται πλήρως με τα υπογεγραμμένα ιδιωτικά έγγραφα (Χριστοδούλου Κ., 2013, σ. 69-73), τα οποία φέρουν ιδιόχειρη υπογραφή. Βάσει αυτού του κριτηρίου λοιπόν τα ηλεκτρονικά έγγραφα διακρίνονται σε ρυθμιζόμενα και «μη ρυθμιζόμενα». Ειδικότερα, δυνάμει του άρθρου 25 παρ. 2 του ισχύοντος Κανονισμού (910/2014/Ε.Ε.) ρυθμιζόμενα είναι τα έγγραφα, τα οποία φέρουν την εγκεκριμένη υπογραφή του εκδότη τους, η οποία δημιουργείται από εγκεκριμένη διάταξη ηλεκτρονικής υπογραφής και βασίζεται σε εγκεκριμένο ηλεκτρονικό πιστοποιητικό. Ωστόσο, ο ίδιος ο Κανονισμός σαφώς ορίζει ότι ακόμα και στην περίπτωση των μη ρυθμιζόμενων εγγράφων, τα οποία δεν πληρούν όλες αυτές τις προϋποθέσεις, η νομική ισχύς και το τυχόν παραδεκτό της ηλεκτρονικής υπογραφής τους (εάν φέρουν) δεν απορρίπτονται μόνο εξ αυτού του λόγου (άρθρο 46 του Κανονισμού (Ε.Ε.) 940/2014).

Συμπερασματικά, το παρόν πόνημα αφορούν τα γνήσια, ρυθμιζόμενα και μη έγγραφα ως «φορείς» δεδομένων, τα οποία εξωτερικεύουν τη βούληση του εκδότη τους στο περιβάλλον του διαδικτύου.

[33] Κοσμάς Α. Καραδημητρίου, ό.π., σ. 36, για τη διάκριση σε γνήσια και μη γνήσια ηλεκτρονικά έγγραφα βλ. και Γ. Ζέκο, ό.π., σ. 73 επ.

Κεφάλαιο 2ο: Ηλεκτρονικές υπογραφές – η έννοια και η λειτουργία τους

Η ανάπτυξη των συναλλαγών στο διαδίκτυο και η εκτεταμένη χρήση των ηλεκτρονικών εγγράφων κατέστησαν απαιτητή εξεύρεσης τρόπου υπογραφής των ηλεκτρονικών εγγράφων. Η ανάγκη αυτή έγκειται αφενός στους σκοπούς διασφάλισης των ηλεκτρονικών επικοινωνιών και συναλλαγών όπως ανωτέρω αναλύθηκε,[35] αφετέρου δε διαπιστώθηκε η ανάγκη να εξομοιωθεί ρητά το ηλεκτρονικό έγγραφο με το ιδιοχείρως υπογραφόμενο ιδιωτικό έγγραφο, προς αποφυγήν «παρεξηγήσεων».[36]

2.1. Η σημασία της υπογραφής στο ελληνικό ουσιαστικό και δικονομικό δίκαιο

Η υπογραφή αποτελεί εκείνο το έγγραφο στοιχείο δια του οποίου ο εκδότης του εγγράφου δηλώνει την ταυτότητά του.[37] Αυτή δε τίθεται, προκειμένου να δηλωθεί η βούλησή (και πρόθεση) του συντάκτη να δεσμευτεί από το περιεχόμενο του εγγράφου επί του οποίου τίθεται η υπογραφή.[38] Η δε υπογραφή συνίσταται στη θέση του πλήρους ονόματος του υπογράφοντος, ήτοι του κυρίου ονόματος και του επωνύμου, χωρίς να είναι απαραίτητο να περιλαμβάνεται το πατρώνυμο.[39] Αυτή δε, θα πρέπει να είναι ιδιόγραφη, ώστε δια του (μοναδικού) γραφικού χαρακτήρα να μπορεί να μπορεί επιβεβαιωθεί η ταυτότητα του υπογράφοντος.

Η ιδιαίτερη σημασία που έχει η υπογραφή του εγγράφου από τον εκδότη του γίνεται αντιληπτή από τη σημασία που της προσδίδει ο Έλληνας νομοθέτης. Ειδικότερα, για τις δικαιοπραξίες, για τις οποίες έχει συμφωνηθεί έγγραφος τύπος (άρθρο 160 ΑΚ), θα πρέπει ο εκδότης αυτού να έχει θέσει την ιδιόχειρη υπογραφή του, ώστε να καθίσταται αδιαμφισβήτητο ότι όσες πληροφορίες περιέχονται στο κείμενο συνιστούν εκπεφρασμένη βούληση του. Μάλιστα, υπό περιστάσεις καθίσταται απαιτητό η υπογραφή να έχει τεθεί σε πολλαπλά σημεία του εγγράφου, ώστε να γίνει δεκτό ότι ο εκδότης δεσμεύεται από αυτό.[40]

Στο δε χώρο του δικονομικού αστικού δικαίου, κατ' άρθρο 443 ΚΠολΔ ως προς την αποδεικτική ισχύ των ιδιωτικών εγγράφων απαιτείται αυτά να φέρουν την ιδιόγραφη υπογραφή του εκδότη ή τουλάχιστον διακριτικό σημάδι του τελευταίου επικυρωμένο από αρμόδια αρχή. Η θέση υπογραφής, δηλαδή, σε ιδιωτικό έγγραφο αφορά το νόμιμο τύπο που θα πρέπει να έχει ακολουθηθεί, προκειμένου αυτό να δεσμεύσει το κρίνον δικαστήριο για τα όσα δηλώνονται στο σώμα του εγγράφου, χωρίς όμως η δικαστική αρχή να δεσμεύεται να δεχτεί αυτά και ως

---

[35] Βλ. Εισαγωγή, σ. 27.
[36] Βλ. Κωνσταντίνο Χριστοδούλου, 2001, ό.π., σ. 1
[37] Ι. Λιναρίτης, Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών μετά την ενσωμάτωση της Οδηγίας 99/93 της ΕΕ στο ελληνικό δίκαιο με το ΠΔ 150/2001, ΔΕΕ. 3/2002, σ. 257
Κωνσταντίνος Χριστοδούλου (2000) , ό.π. , σ. 1
[38] Χ. Μιχαηλίδου, ό.π., σ. 2
[39] ΕφΠατρ 143/2008
[40] Χ. Μιχαηλίδου, ό.π., σ. 3-4

αληθή.[41] Μάλιστα, έχει επισημανθεί ότι «μ' αυτήν την προϋπόθεση το ιδιωτικό έγγραφο έχει την ιδιαίτερη αποδεικτική δύναμη που ορίζει το άρθρο 445 ΚΠολΔ, δηλαδή ότι το δικαστήριο δεσμεύεται να δεχτεί πως η περιεχόμενη στο ιδιωτικό έγγραφο δήλωση προέρχεται από τον αναφερόμενο ως εκδότη του υπογραφέα**.** Δεν πρέπει λοιπόν να υπερτιμάται η αποδεικτική ισχύς του ιδιωτικού εγγράφου, αφού, σ' αντίθεση προς τα δημόσια έγγραφα (πρβλ. 441 ΚΠολΔ), τα ιδιωτικά έγγραφα δεν δεσμεύουν όσον αφορά το αληθές του περιεχομένου σ' αυτά δηλώσεων αλλά μόνον όσον αφορά το ότι οι δηλώσεις προέρχονται από τον εκδότη του ιδιωτικού εγγράφου. Αυτό σημαίνει ότι το ιδιωτικό έγγραφο αποδεικνύει δεσμευτικώς αποκλειστικά και μόνον ότι ο εκδότης του έκανε την περιεχόμενη σ' αυτό εξώδικη ομολογία (πρβλ. ΚΠολΔ 447), η οποία όμως, ως αυτοτελές αποδεικτικό μέσο, εκτιμάται ελευθέρως (ΚΠολΔ 352 § 2).».[42] Τέλος, θα πρέπει να σημειωθεί ότι ιδιαίτερης σημασίας εν προκειμένω είναι το ιδιόγραφο της υπογραφής, το οποίο θα πρέπει να μην μπορεί να αμφισβητηθεί ενώπιον του δικαστηρίου, ή σε κάθε περίπτωση αυτό να μπορεί να αποδειχθεί πέραν αμφιβολίας.[43]

Τέλος, για λόγους πλήρους αντίληψης της σημασίας των υπογραφών ακροθιγώς σημειώνεται ότι στη σφαίρα του Διοικητικού Δικαίου, κατ' άρθρο 16 ΚΔΔιαδ., η υπογραφή του εκδότη αποτελεί στοιχείο του υποστατού της ίδιας της πράξης, οπότε και έλλειψή της καθιστά την πράξη ανυπόστατη, ως ατελή. Το δε όργανο της δημοσιευτέας πράξης θα πρέπει να είναι αρμόδιο, τόσο κατά το χρόνο υπογραφής της, όσο και δημοσίευσής της, ενώ επί συλλογικού οργάνου αρκεί η υπογραφή του προέδρου του (άρθρο 15 παρ. 8 ΚΔΔιαδ.). Εάν επί του αντιγράφου της προσβαλλόμενης πράξης, δίπλα στη θέση υπογραφής του εκδόντος αυτή οργάνου που αναγράφεται με μηχανικό μέσο, περιέχεται σφραγίδα με την οποία βεβαιώνεται η ακρίβεια του αντιγράφου και η οποία φέρει ημερομηνία και χειρόγραφη υπογραφή δημοσίου υπαλλήλου, με τον τρόπο αυτό βεβαιώνεται ότι το πρωτότυπο της προσβαλλόμενης πράξης φέρει την υπογραφή του αρμοδίου οργάνου.[44].

2.2. Εννοιολογική προσέγγιση της ηλεκτρονικής υπογραφής

Όπως ήδη έχει αναφερθεί, η ανάπτυξη των τεχνολογιών και δη του διαδικτύου, μαζί με την παροχή νέων δυνατοτήτων, έφερε τους χρήστες του αντιμέτωπους με την ανάγκη να

[41] ΑΠ 2064/2006 & ΑΠ 3/2001

[42] Κώστας Μπέης σε μελέτη-παρατηρήσεις στη νομολογία, ΠολΔ 623.- Διαταγή πληρωμής βάσει ηλεκτρονικού εγγράφου, Δ. 2001, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=1479&mnu=3&id=17912, (ημερομηνία επίσκεψης 25-04-2020)

[43] ΑΠ 3/2001, Δ. 2001, με ενημ. σημ. Κ.Ε.Μ. διαθέσιμο στην ηλεκτρονική σελίδα http://www.kostasbeys.gr/articles.php?s=5&mid=&mnu=0&id=18031&keyw=%C1%D0+3%2F2001&sr=search&pg= (τελευταία επίσκεψη 10-04-2020)

[44] Κωνσταντίνος Γώγος, Η ανυπόστατη διοικητική πράξη, Εκδόσεις Σάκκουλας: Αθήνα-Θεσσαλονίκη 2012, σ. 148-150

ανταποκριθούν στις νέες συνθήκες επικοινωνίας, αλλά και συναλλαγών. Η χρήση ηλεκτρονικών μέσων και δη ηλεκτρονικών εγγράφων κατέστησε αδήριτη την ανάγκη να βρεθεί εκείνο το ισοδύναμο μέσο της ιδιόχειρης υπογραφής, το οποίο θα μπορεί κατά το μέγιστο βαθμό να εξασφαλίζει τις προϋποθέσεις ασφάλειας που απαιτούνται κατά τις ηλεκτρονικές συναλλαγές (αυθεντικότητα-authentication, ακεραιότητα-integrity, εμπιστευτικότητα-confidentiality, μη αποποίηση ευθύνης-non repudation).

Ήδη από το 1998, οπότε και δημοσιεύτηκε ο ν. 2672/1998 («Οικονομικοί πόροι της Νομαρχιακής Αυτοδιοίκησης και άλλες διατάξεις», ΦΕΚ 290 Α/28-12-1998), ο Έλληνας νομοθέτης επιχειρεί, για χάρη της διοίκησης και της διακίνησης εγγράφων μέσω ηλεκτρονικού ταχυδρομείου και τηλεομοιοτυπίας (σε εκείνη την περίπτωση), να προσεγγίσει για πρώτη φορά (στην ελληνική έννομη τάξη) τον ορισμό της ηλεκτρονική υπογραφής. Ειδικότερα, στο άρθρο 14 παρ. 2 στοιχ. ε οριζόταν ως ψηφιακή υπογραφή «η ψηφιακής μορφής υπογραφή σε δεδομένα ή συνημμένη σε δεδομένα ή λογικά συσχετιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη αποδοχής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή: αα) συνδέεται μονοσήμαντα με τον υπογράφοντα, ββ) ταυτοποιεί τον υπογράφοντα, γγ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και δδ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.». Ο νομοθέτης μετατόπισε το βάρος του ορισμού στο σκοπό που αυτή όφειλε να εξυπηρετεί. Τις ίδιες προϋποθέσεις αργότερα θα έθετε και ο τότε κοινοτικός (νυν ενωσιακός) νομοθέτης με την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ως ιδιότητες, όχι εν γένει των ηλεκτρονικών υπογραφών, αλλά ως απαιτήσεις της «προηγμένης ηλεκτρονικής υπογραφής»[45], οι οποίες (ιδιότητες) διατηρούνται και σήμερα στον ισχύοντα Κανονισμό (Ε.Ε.) 9140/2014.[46]

[45] άρθρο 2 περ. 2 της Οδηγία 99/93/Ε.Κ.: «προηγήθη ηλεκτρονική υπογραφή»: ηλεκτρονική υπογραφή που ανταποκρίνεται στις εξής απαιτήσεις: α) συνδέεται μονοσήμαντα με τον υπογράφοντα· β) είναι ικανή να ταυτοποιήσει τον υπογράφοντα· γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπάρει να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και δ) συνδέεται με τα δεδηγμένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.», βλ. και Χ. Σιούλης Η ευρωπαϊκή νουθεσία για τις ηλεκτρονικές υπογραφές (Ανάλυση και Σχολιασμός), 2003, σ. 11 και υποσημείωση 24, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/El-Sign_Directive2.pdf (ημερομηνία επίσκεψης 10-02-2020]

[46] άρθρο 3 στοιχ. 11 του Κανονισμού (Ε.Ε.) 910/2014: «προηγμένη ηλεκτρονική υπογραφή»: ηλεκτρονική υπογραφή που ανταποκρίνεται στις απαιτήσεις του άρθρου 26·», ενώ το άρθρο 26 αναφέρει: «Μία προηγμένη ηλεκτρονική υπογραφή πληροί τις ακόλουθες απαιτήσεις: α) συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα· β) είναι ικανή να ταχτοποιεί τον υπογράφοντα· γ) δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο, και δ) συνδέεται με τα δεδομένα που έχουν υπογραφεί σε

Με τη θέση σε ισχύ της Οδηγίας 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για να διευκολυνθεί η χρήση ηλεκτρονικών υπογραφών και να ενισχυθεί η νομική αναγνώρισή τους[47] και προκειμένου για την ενίσχυση της ασφάλειας της εσωτερικής αγοράς της Κοινότητας στα πλαίσια των ραγδαίως αναπτυσσόμενων συναλλαγών μέσω διαδικτύου[48] δόθηκε εκ νέου ο ορισμός της ηλεκτρονικής υπογραφής. Τον ορισμό αυτό υιοθέτησε δε πλήρως και ο Έλληνας νομοθέτης με το π.δ. 150/2001, το οποίο και ενσωμάτωσε τις διατάξεις της Οδηγία 99/93/Ε.Κ.. Στο άρθρο 2 παρ. 1 ορίζεται ότι ως ηλεκτρονική υπογραφή νοούνται «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας».

Ωστόσο, από το θέση σε ισχύ της εν λόγω Οδηγία 99/93/Ε.Κ., η ανάπτυξη του ψηφιακού ή αλλιώς επιγραμμικού περιβάλλοντος και η ανάγκη ενίσχυσης των σχέσεων εμπιστοσύνης σε συνδυασμό με την ανάπτυξη της τεχνολογίας, οδήγησαν την Ευρωπαϊκή Ένωση στη δημοσίευση του Κανονισμού eIDAS (Κανονισμός 910/2014/Ε.Ε), με τον οποίο καταργήθηκε η προαναφερθείσα Οδηγία 99/93/Ε.Κ.. Έτσι, προστρέχοντας κανείς στον ισχύοντα Κανονισμό για την προσέγγιση της έννοιας της ηλεκτρονικής υπογραφής παρατηρεί πλέον (άρθρο 3 στοιχ. 10) ότι ως ηλεκτρονική υπογραφή ορίζεται το σύνολο δεδομένων σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή, αλλά πλέον τα δεδομένα αυτά χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει (σε ηλεκτρονική μορφή).

2.3. Ο σκοπός της ηλεκτρονικής υπογραφής

Από τον ανωτέρω ορισμό προκύπτει ότι ο όρος ηλεκτρονικές υπογραφές, άλλοτε χρησιμοποιείται για να περιγράψει τα συνημμένα δεδομένα και άλλοτε για να περιγράψει τη διαδικασία διασφαλίσεως-τεκμηρίωσης με ηλεκτρονικά μέσα (security procedure).[49]. Η τυχόν εννοιολογική προσέγγιση βέβαια της τελευταίας περίπτωσης θα πρέπει να προσεγγίζεται με τελολογικά κριτήρια. Η ανάγκη ασφαλούς επικοινωνίας, αλλά και ασφαλών συναλλαγών στο χώρο του διαδικτύου θα πρέπει να διασφαλίζεται εξίσου. Και τούτο επιτυγχάνεται μέσω των συνημμένων δεδομένων που συνιστούν την ηλεκτρονική υπογραφή.[50] Ταυτόχρονα όμως με τις

σχέση με αυτήν κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.»

[47] Βλ. και άρθρο 1 της Οδηγίας (Ε.Κ.) 99/93: «Στόχος της παρούσας οδηγίας είναι να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους. Θεσπίζει νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την άλαλη λειτουργία της εσωτερικής αγοράς»

[48] Αιτιολογικές σκέψεις 5-8 του προοιμίου της Οδηγίας (Ε.Κ.) 99/93

[49] Κορνηλία Δελούκα-Ιγγλέση, , υπ., σ. 185, βλ. και Γ. Ζέκο, υπ., σ. 84, όπου αναφέρεται στις ηλεκτρονικές υπογραφές ως το τεχνολογικό μέσο που αξιοποιείται (αλγόριθμο) και όχι ως τη διαδικασία διασφαλίσεως.

[50] Α. Παπαθωμά–Μπέτγκε ό.π. 1241-1242

ηλεκτρονικές υπογραφές επιδιώκεται η βεβαιότητα του παραλήπτη του ηλεκτρονικού μηνύματος ότι το περιεχόμενο (άρα και η όποια εκπεφρασμένη εντός αυτού βούληση) ανήκει στον εκδότη-αποστολέα, χωρίς αυτή να έχει τροποποιηθεί ή αλλοιωθεί από τρίτους.[51]

Υπό το ανωτέρω πρίσμα, καταλήγει κανείς στο συμπέρασμα ότι δεν αρκούν οποιαδήποτε ηλεκτρονικά δεδομένα, συνημμένα σε άλλα, αλλά εκείνα, τα οποία επιτρέπουν να ακολουθηθεί μια διαδικασίας επαλήθευσης. Έτσι, παρά τις αντίθετες φωνές[52] έχει υποστηριχθεί από τη θεωρία ότι δεν μπορεί να θεωρηθεί ως ηλεκτρονική υπογραφή τυχόν επικόλληση της ηλεκτρονικής αποτύπωσης ιδιόχειρης υπογραφής με τη χρήση τεχνικών μέσων, όπως ένας σαρωτής (scanner).[53] Πέραν της προφανούς αποκλίσεως μεταξύ της έννοιας (ηλεκτρονικής) επικόλλησης και σύναψης (συνένωσης δηλαδή), μία τέτοια πρακτική επιτρέπει να εμφιλοχωρήσουν κίνδυνοι, όπως αλλοίωσης του περιεχομένου, πλαστογραφίας ή και υποκλοπής. Τουναντίον, όπως εντόνως έχει επισημανθεί[54], τα δεδομένα της ηλεκτρονικής υπογραφής θα πρέπει να είναι κωδικοί-απόρρητα στοιχεία του υπογράφοντος, τα οποία, συνημμένα στο ηλεκτρονικό έγγραφο, θα συνιστούν μία «κλειδωμένη» σύντμηση που θα λειτουργεί ως δακτυλικό αποτύπωμα του ηλεκτρονικού εγγράφου.

Ανακεφαλαιώνοντας λοιπόν, υπό το πρίσμα του ισχύοντος Κανονισμού, με τον όρο ηλεκτρονική υπογραφή αναφέρεται κανείς σε εκείνα τα δεδομένα, τα οποία συνιστούν απόρρητα στοιχεία (κωδικούς) του υπογράφοντος-συντάκτη του ηλεκτρονικού εγγράφου και τα οποία, συνημμένα σε άλλα ηλεκτρονικά δεδομένα (ηλεκτρονικά έγγραφα), πρόκειται όχι μόνο να επιτελέσουν τις λειτουργίες της ιδιόγραφης υπογραφής αλλά και να «θωρακίσουν» το έγγραφο από πάσης φύσεως κακόβουλες ενέργειες τρίτων. Αυτός είναι άλλωστε και ο λόγος για τον οποίο η νομική θεωρία - ήδη με τα δεδομένα του προϊσχύσαντος νομικού καθεστώτος - προσδιόρισε την ηλεκτρονική υπογραφή ως «τη μέθοδο τεκμηρίωσης με ηλεκτρονικά μέσα (security procedure) που χρησιμοποιείται σε συγκεκριμένες μηχανικές απεικονίσεις (εγγραφές δεδομένων σε μαγνητικά μέσα ηλεκτρονικού υπολογιστή, συμπεριλαμβανομένης της ηλεκτρονικής ανταλλαγής δεδομένων και της ηλεκτρονικής αλληλογραφίας) με σκοπό να διασφαλίσει αφενός τη γνησιότητα και ακρίβεια δήλωσης βουλήσεως που περιέχουν και αφετέρου τα στοιχεία του προσώπου που προβαίνει στη δήλωση αυτή».

[51] Μητρακάς Α., Οι ηλεκτρονικές υπογραφές στο ευρωπαϊκό και ελληνικό δίκαιο: Ζητήματα εφαρμογών στον τραπεζικό τομέα. Δελτίο ΕΕΤ εξάμηνο 2003, σ. 109 διαθέσιμο στην ηλεκτρονική διεύθυνση https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/3_2003.pdf (ημερομηνία επίσκεψης 03-04-2020)
[52] Φιλιπποπούλου Ε.(200).Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου. ΔΕΕ 11/2000, σ. 1091, βλ. και Γ. Ζέκο, ό.π. σ. 84επ.
[53] Α Παπαθωμά–Μπέτγκε., ό.π. σ. 1241-1242, Χ. Μιχαηλίδου, ό.π., σ. 3
[54] Κορνηλία Δελούκα-Ιγγλέση, ό.π., σ. 183

Κεφάλαιο 3ο: Οι κατηγορίες των ηλεκτρονικών υπογραφών

Στο παρόν κεφάλαιο εξετάζονται οι κατηγορίες των ηλεκτρονικών υπογραφών. Στην πρώτη ενότητα παρουσιάζονται οι διακρίσεις με βάση τη μέθοδο που ακολουθείται για την δημιουργία τους. Στη συνέχεια παρουσιάζονται οι διακρίσεις των ηλεκτρονικών υπογραφών, όπως αυτές εντοπίζονται στον Κανονισμό 910/20114, ενώ ενδελεχής αναφορά γίνεται και στις προϋποθέσεις που τάσσει ο Κανονισμός (Ε.Ε.) 910/2014 για την εγκυρότητά τους. Δεν παραλείπεται δε κατά την ανάλυσή τους η αναφορά και στις απόψεις της θεωρίας που υποστηρίχτηκαν κατά το προϊσχύον δίκαιο και τυγχάνουν εφαρμογής και υπό τις ισχύουσες διατάξεις.

3.1. Τα είδη της ηλεκτρονικής υπογραφής με κριτήριο τη μέθοδο δημιουργίας που χρησιμοποιείται.

Ήδη αναλύθηκε, όχι μόνο η φύση της ηλεκτρονικής υπογραφής, αλλά πολύ περισσότερο και η λειτουργία που αυτή καλείται να επιτελέσει. Τόσο στα πλαίσια του ισχύοντος Κανονισμού[55], όσο και στην καθημερινή πρακτική έχουν υπάρξει διάφορα είδη είτε στοιχείων, είτε κωδικών – απόρρητων δεδομένων που χρησιμοποιούνται ως ηλεκτρονικές υπογραφές.

Σκόπιμο κρίνεται, όπως εξεταστούν πρώτα οι περιπτώσεις εκείνες που πληρούν τα περισσότερα κριτήρια ασφαλείας, ήτοι όταν πρόκειται για συνάψεις, οι οποίες λειτουργούν πιο αποτελεσματικά ως «δακτυλικό αποτύπωμα» παρέχοντας τα περισσότερα εχέγγυα ασφαλείας. Έτσι, είδος ηλεκτρονικής υπογραφής συνιστά και η εκ των προτέρων γνώση ενός μυστικού κωδικού, όπως στις περιπτώσεις των κωδικών αριθμών PIN.[56] Ωστόσο, η χρήση τους είναι ιδιαίτερα επισφαλής, αφού ο κωδικός αυτός μπορεί να υποκλαπεί. Στον αντίποδα βρίσκονται οι βιομετρικές. Εν προκειμένω αξιοποιούνται μοναδικά βιολογικά χαρακτηριστικά ενός ατόμου (π.χ. ίριδα οφθαλμού, δακτυλικό αποτύπωμα, κ.λπ.), ώστε μέσα σε ελάχιστο χρόνο να ελέγχεται και να αναγνωρίζεται η ταυτότητα του υποκειμένου που τα φέρει[57].

[55] ως κατωτέρω ενότητα 4.2 αναλύεται

[56] Χ. Μιχαηλίδου ό.π.

[57] Σημειωτέον ότι, όλα τα βιομετρικά συστήματα λειτουργούν περίπου με τον ίδιο τρόπο: Καταρχήν το σύστημα «καταγράφει» ένα δείγμα του συγκεκριμένου βιομετρικού χαρακτηριστικού. Στη συνέχεια, εξάγονται τα μοναδικά γνωρίσματα του βιομετρικού χαρακτηριστικού από τα οποία παράγεται μία μαθηματική εξίσωση, από την οποία ακολούθως παράγεται το «βιομετρικό κλειδί», που μπορεί να αποθηκευθεί σε σκληρό δίσκο, «έξυπνη κάρτα» κ.ο.κ. Τελικά, ο έλεγχος της ταυτότητος του χρήστη από το βιομετρικό σύστημα πραγματοποιείται με σύγκριση του δείγματος με το πρότυπο. Τα βιολογικά προσωπικά χαρακτηριστικά ενός ατόμου, ούτε να κλαπούν ούτε να αντιγραφούν ούτε και να ξεχαστούν μπορούν. Για τους λόγους αυτούς η αρχικά δειλή και φειδωλή χρήση τους έχει αρχίσει να αναπτύσσεται με γοργούς ρυθμούς . Δικαίως θεωρούνται ως ένα πολλά υποσχόμενο είδος ηλεκτρονικής υπογραφής. Βλ. Κορνηλία Δελούκα – Ιγγλέση, ό.π., σ. 192-195.

Διακριτή περίπτωση, η οποία ενδελεχώς εξετάζεται αμέσως κατωτέρω, αφορά στις περιπτώσεις των ηλεκτρονικών υπογραφών που στηρίζονται σε μεθόδους της κρυπτογραφίας.

3.1.1. Η ηλεκτρονική υπογραφή με βάση την κρυπτογραφία.

Η κρυπτογραφία είναι η επιστήμη που σκοπό της έχει την προστασία των δεδομένων και η οποία παρέχει μέσα και μεθόδους για τη μετατροπή των δεδομένων σε μη αναγνώσιμη μορφή. Στόχος της επιστήμης αυτής είναι η αποτροπή πρόσβασης σε δεδομένα από μη εξουσιοδοτημένους χρήστες, καθιστώντας το περιεχόμενό τους κρυφό.[58]

Μάλιστα, ακόμα και ο κοινοτικός νομοθέτης επιχειρώντας να επαναπροσδιορίσει τους όρους του Παραρτήματος Ι του κανονισμού 1334/2000, δια του Κανονισμού (Ε.Κ.) 149/2003 του Συμβουλίου περί κοινοτικού συστήματος ελέγχου των εξαγωγών ειδών και τεχνολογίας διπλής χρήσης, υιοθέτησε τον ακόλουθο ορισμό «(ημερομηνία επίσκεψης κρυπτογραφία] είναι ο κλάδος που συνδυάζει τις αρχές, τα μέσα και τις μεθόδους για την μετατροπή δεδομένων με σκοπό την απόκρυψη των πληροφοριών που περιέχουν, την πρόληψη της μη αντιληπτής τροποποίησής τους ή της μη επιτρεπτής χρήσης τους. Η κρυπτογραφία περιορίζεται στην μετατροπή πληροφοριών χρησιμοποιώντας μία ή περισσότερες μυστικές παραμέτρους (π.χ. κρυπτομεταβλητές) ή σχετική διαχείριση κλειδιών.»

Δεδομένων των στόχων που επιτυγχάνονται μέσω της κρυπτογραφίας, αυτή αξιοποιείται ως το τεχνολογικό μέσον για να παρέχεται ασφάλεια κατά τη διαβίβαση δεδομένων σε πληροφοριακά και επικοινωνιακά συστήματα. Είναι ιδιαίτερα σημαντική σε περιπτώσεις προσωπικών και οικονομικών δεδομένων, ανεξαρτήτως αν για τη διαβίβαση αυτών έχει γίνει χρήση κάποιου μέσου ή συσκευής αποθήκευσης. Μάλιστα, αξίζει να σημειωθεί ότι με τους αλγόριθμους που χρησιμοποιούνται κατά την κρυπτογραφία μπορεί να επιτευχθεί ταυτόχρονα ο έλεγχος γνησιότητας των δεδομένων αλλά και ο εντοπισμός τυχόν τροποποίησής τους. Συνακόλουθα, καθίσταται εφικτό ο αποστολέας/δημιουργός του εκάστοτε μηνύματος των δεδομένων να δεσμεύεται από αυτό και να μην μπορεί να το αποκηρύξει.

Βασικοί όροι[59] για την κατανόηση των μεθόδων ψηφιακής κρυπτογραφίας είναι:

- Αρχικό κείμενο (plaintext) είναι το αρχικό μήνυμα που θα διαβιβαστεί στον παραλήπτη
- Κρυπτοθέτηση (encryption) ονομάζεται η διαδικασία της τροποποίησης του περιεχομένου ενός μηνύματος με τρόπο τέτοιο που να αποκρύπτεται το πραγματικό μήνυμα
- Κρυπτογραφημένο κείμενο (ciphertext) είναι το αποτέλεσμα της κρυπτογράφησης του αρχικού κειμένου

[58] Choudhury, S (Ed.). Public Key Infrastructure Implementation and Design. New York: D. M&T Books, 2002, σ. 11
[59] Choudhury, ό.π.,σ. 12

- Αποκρυπτογράφηση (decryption) είναι η αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή η ανάκτηση του αρχικού κειμένου από το κρυπτογραφημένο κείμενο.
- Κλειδί (key) ονομάζεται μία λέξη, γράμμα ή φράση η οποία χρησιμοποιείται για την κρυπτογράφηση του αρχικού κειμένου. Στη σύγχρονη κρυπτογραφία που βασίζεται στους υπολογιστές, οποιοδήποτε κείμενο, λέξη-κλειδί ή φράση μετατρέπεται με τη χρήση αλγορίθμων σε ένα μοναδικό συνδυασμό από γράμματα και αριθμούς. Το αποτέλεσμα αυτής της μετατροπής χρησιμοποιείται ως κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση.

Για την κρυπτογράφηση και μετέπειτα αποκρυπτογράφηση οποιουδήποτε μηνύματος με αυτή τη μέθοδο χρειάζεται ένα κλειδί. Στον τρόπο διαχείρισης αυτού του κλειδιού λοιπόν έγκειται η διαφορά ανάμεσα στις δύο βασικές κατηγορίες κρυπτογραφίας που υπάρχουν. Αυτές είναι η συμμετρική (symmetric) κρυπτογραφία ή κρυπτογραφία ιδιωτικού κλειδιού (private key) και η κρυπτογραφία δημοσίου κλειδιού (public key) ή ασύμμετρη κρυπτογραφία.

3.1.1.1. Η ηλεκτρονική υπογραφή που στηρίζεται στη συμμετρική κρυπτογραφία

Η συμμετρική κρυπτογραφία βασίζεται στην ύπαρξη ενός και μόνο κλειδιού το οποίο χρησιμοποιείται τόσο κατά την διαδικασία της κρυπτογράφησης, όσο και κατά την διαδικασία της αποκρυπτογράφησης. Ο αποστολέας του μηνύματος κρυπτογραφεί το αρχικό κείμενο με τη χρήση του κλειδιού αυτού και αποστέλλει το μήνυμα στον παραλήπτη. Για να είναι δυνατή η αποκρυπτογράφηση ωστόσο στο αρχικό μήνυμα είναι αναγκαία η γνώση του κλειδιού αυτού. Ο παραλήπτης λοιπόν και ο αποστολέας πρέπει να έχουν το ίδιο κλειδί. Η διαδικασία απόκτησης του κλειδιού αυτού από τον παραλήπτη είναι γνωστή και ως ανταλλαγή κλειδιού (key exchange) και αποτελεί ολόκληρο υποκλάδο στην επιστήμη της κρυπτογραφίας. Από τα παραπάνω συμπεραίνουμε ότι η κατοχή του κρυπτογραφημένου μηνύματος από τρίτους χωρίς την ταυτόχρονη κατοχή και του κλειδιού κρυπτογράφησης διασφαλίζει το απόρρητο της επικοινωνίας καθώς η ανάκτηση του αρχικού μηνύματος δεν είναι δυνατή. Η βασικότερη αδυναμία της συμμετρικής κρυπτογραφίας έγκειται στην χρήση ενός και μόνο κλειδιού.[60] Αν το κλειδί αυτό γίνει γνωστό σε κάποιον τρίτο πέραν των αποστολέα και παραλήπτη του μηνύματος, τότε υπάρχει πολύ μεγάλος κίνδυνος. Το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί και να αποκαλύψει το περιεχόμενό του. Επιπλέον, λόγω του ότι το κλειδί αυτό χρησιμοποιείται τόσο κατά την κρυπτογράφηση όσο και κατά την αποκρυπτογράφηση, θα ήταν δυνατό σε όποιον τρίτο γνωρίζει το κλειδί να ανακτήσει το αρχικό μήνυμα από το κρυπτογραφημένο, να το τροποποιήσει και μετά να το κρυπτογραφήσει και να αποστείλει το νέο τροποποιημένο μήνυμα. Ένας επιπλέον κίνδυνος που υπάρχει στη συμμετρική κρυπτογράφηση είναι ότι η ταυτότητα του αποστολέα δεν μπορεί να γίνει γνωστή στον

[60] Andress J., The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition. Oxford: Elsevier Inc. 2014. σ. 76

παραλήπτη. Έτσι ο παραλήπτης δεν μπορεί να εξακριβώσει αν το μήνυμα προέρχεται από τον αποστολέα που επιθυμεί ή από κάποιον τρίτο που έχει υποκλέψει την ψηφιακή ταυτότητα του αποστολέα. Παρά τις αδυναμίες που έχει η συμμετρική κρυπτογράφηση, υπάρχουν αρκετοί αλγόριθμοι κρυπτογράφησης με κυριότερους εξ αυτών τους DES, 3DES, AES, εκ των οποίον ειδικά ο AES χρησιμοποιείται ακόμα και σήμερα.[61]

Συνεπώς, η αξιοποίηση της συμμετρικής κρυπτογραφίας και του ιδιωτικού κλειδιού για την υπογραφή ηλεκτρονικών εγγράφων μπορεί να οδηγεί στην επιθυμητή «σύναψη» δεδομένων, παραμένει όμως εκτεθειμένη σε κινδύνους υποκλοπής σε περίπτωση που το ιδιωτικό κλειδί γίνει γνωστό σε περισσότερους, πέραν των άμεσα ενδιαφερομένων. Για αυτό το λόγο, άλλωστε, η χρήση ηλεκτρονικών υπογραφών που στηρίζονται σε αυτή τη μέθοδο συστήνεται στο πλαίσιο ενός μικρού δικτύου κοινωνών ή στο πλαίσιο ενός κλειστού δικτύου (πχ: στα πλαίσια λειτουργίας μίας εταιρείας).

Ωστόσο, τα σημαντικότερα προβλήματα της συμμετρικής κρυπτογραφίας λύνονται με την κρυπτογραφία δημοσίου κλειδιού ή αλλιώς την ασύμμετρη κρυπτογραφία, την οποία εξετάζουμε αμέσως πιο κάτω.

3.1.1.2. Η υπογραφή που στηρίζεται στην ασύμμετρη κρυπτογραφία

Σε αντίθεση με τη συμμετρική κρυπτογραφία, στην ασύμμετρη κρυπτογραφία (ή αλλιώς συχνά αποκαλούμενη RSA εκ των αρχικών των δημιουργών της) δημόσιου κλειδιού δεν χρησιμοποιείται ένα μοναδικό κλειδί, αλλά ένα ζεύγος κλειδιών. Στο ζεύγος αυτό, το ένα κλειδί ονομάζεται ιδιωτικό (private) και το άλλο δημόσιο (public). Τα δύο κλειδιά είναι μαθηματικώς συσχετιζόμενα μεταξύ τους και για το μαθηματικό μοντέλο δημιουργίας τους χρησιμοποιείται η θεωρία πρώτων αριθμών.[62] Ο αποστολέας του μηνύματος αποθηκεύει και κρατάει μυστικό το ιδιωτικό κλειδί ενώ το δημόσιο κλειδί γίνεται ελεύθερα προσβάσιμο σε οποιονδήποτε μπορεί να έχει κάποια συναλλαγή με τον ιδιοκτήτη του. Τονίζεται δε ότι η μέθοδος δημιουργίας του δημόσιου κλειδιού «είναι μονόδρομη συνάρτηση του ιδιωτικού», ήτοι δεν είναι εφικτό μέσω του τελευταίου να προσδιοριστεί ποιο είναι το ιδιωτικό κλειδί.[63]

Τα δύο αυτά κλειδιά λειτουργούν ως ζεύγος με τον εξής τρόπο. Κατά τη διαδικασία κωδικοποίησης ενός μηνύματος χρησιμοποιείται το ιδιωτικό κλειδί, το οποίο είναι γνωστό μόνο στον κάτοχό του. Το κρυπτογραφημένο μήνυμα που προκύπτει μπορεί να αποκρυπτογραφηθεί

---

[61] Choudhury, S (Ed.), ό.π. σ.13-18

62 Bose S. and Vijayakumar P. Cryptography and Network Security. Chennai: Pearson India Education Services Pvt.,2016, σ. 205-206

63 Κ. Δελούκα-Ιγγλέση, ό.π. σ. 190

μόνο με τη χρήση του αντίστοιχου δημοσίου κλειδιού. Πλέον ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κωδικοποιήσει το αρχικό μήνυμα. Όταν αυτό φτάσει στον παραλήπτη, αυτός με τη χρήση του ιδιωτικού κλειδιού μπορεί να το αποκρυπτογραφήσει. Λόγω του ότι το δημόσιο κλειδί είναι προσβάσιμο από όλους τους χρήστες, δεν χρειάζεται να γίνει κάποια ανταλλαγή κλειδιού η οποία να είναι ευάλωτη σε υποκλοπή. Επίσης, ο αποστολέας γνωρίζει ότι μόνο ο πραγματικός παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα αφού μόνο αυτός κατέχει το ιδιωτικό κλειδί. Η πολυπλοκότητα του αλγορίθμου δημιουργίας του ζεύγους ιδιωτικού – δημόσιου κλειδιού εξασφαλίζει ότι μέχρι στιγμής δεν υπάρχει τρόπος να μπορεί να υπολογιστεί το ιδιωτικό κλειδί από το δημόσιο κλειδί.[64]

Ωστόσο, η μέθοδος αυτή, ειδικά στις περιπτώσεις εκτενών εγγράφων καθιστά όχι μόνο χρονοβόρα τη σύναψη των δεδομένων υπογραφής, αλλά πολύ περισσότερο ενδέχεται να προκύψουν κρυπτογραφημένα κείμενα, τόσο εκτενούς μορφής που να καθίσταται δυσχερής ακόμα και η αποστολή τους. Στο πρόβλημα αυτό λύση προσφέρει η διαδικασία hashing, η οποία αξιοποιεί συγκεκριμένους αλγόριθμους που διασφαλίζουν την επαλήθευση της γνησιότητας της αποστολής ενός κωδικοποιημένου μηνύματος.[65] Ειδικότερα, με αυτή τη μέθοδο αποστέλλεται ένα κείμενο σε έναν παραλήπτη, ενώ «τροφοδοτείται» από έναν hashing αλγόριθμο το έγγραφο. Ο αλγόριθμος δημιουργεί ένα μοναδικό μικρότερο hashed έγγραφο, το οποίο δεν μπορεί να επανέλθει στο προηγούμενο μέγεθος. Εκτός από το κρυπτογραφημένο έγγραφο λοιπόν, αποστέλλεται σε δεύτερο χρόνο και το hashed έγγραφο. Ο παραλήπτης, αφού αποκρυπτογραφήσει το κρυπτογραφημένο έγγραφο, τροφοδοτεί τον ίδιο αλγόριθμο (hashing). Αν το αρχικό αρχείο δεν έχει αλλοιωθεί από κάποιον ενδιάμεσα, ο αλγόριθμος θα πρέπει να παράξει ένα έγγραφο πανομοιότυπο με το hashed έγγραφο που του έχουμε αποστείλει. Συγκρίνοντας το αποτέλεσμα με το απεσταλμένο hashed έγγραφο μπορεί ο παραλήπτης να είναι σίγουρος ότι το έγγραφο δεν έχει αλλοιωθεί.

Η διαδικασία δημιουργίας μίας ηλεκτρονικής υπογραφής αξιοποιώντας αλγορίθμους hashing από την πλευρά του αποστολέα περιλαμβάνει τα παρακάτω βήματα:

1. Ο αποστολέας δημιουργεί το αρχικό αρχείο που θέλει να αποστείλει.
2. Εκτελώντας έναν αλγόριθμο hash δημιουργεί από το αρχικό αρχείο το hashed αρχείο.
3. Κωδικοποιεί το hashed αρχείο με τη χρήση του ιδιωτικού κλειδιού του.
4. Προσθέτει στο αρχικό αρχείο το κωδικοποιημένο hashed αρχείο.

[64] Andress J. , ό.π., σ 78
[65] Choudhury, S , ό.π., σ. 24

5. Κωδικοποιεί το νέο αρχείο που προέκυψε με τη χρήση του δημοσίου κλειδιού του παραλήπτη.

6. Αποστέλλει το αρχείο στον παραλήπτη.

Από τη μεριά του ο παραλήπτης, για να πιστοποιήσει την ηλεκτρονική υπογραφή, πρέπει να ακολουθήσει τα παρακάτω βήματα:

1. Αποκωδικοποιεί το αρχείο που παρέλαβε με το ιδιωτικό κλειδί του. Το αποκωδικοποιημένο αυτό αρχείο θα περιλαμβάνει το αρχικό κείμενο σε αναγνώσιμη μορφή καθώς και το κωδικοποιημένο hashed αρχείο.

2. Αποκωδικοποιεί το hashed αρχείο με το δημόσιο κλειδί του αποστολέα.

3. Εκτελεί τον ίδιο αλγόριθμο hash στο αρχικό αρχείο. Αν το παραγόμενο hashed αρχείο συμπίπτει με το αποκρυπτογραφημένο hashed αρχείο, τότε βεβαιώνεται η εγκυρότητα του απεσταλμένου αρχείου.

Η χρήση του ζεύγους κλειδιών στην ασύμμετρη κρυπτογραφία λύνει τα προβλήματα που παρουσιάζονταν στη συμμετρική, ενώ με την αξιοποίηση των αλγορίθμων της διαδικασίας hashing, όχι μόνο εξασφαλίζεται η ταχύτητα κατά την μετατροπή των αρχείων, αλλά διασφαλίζεται έτι περαιτέρω το αναλλοίωτο το εγγράφου. Ωστόσο, όπως γίνεται κατανοητό από τα παραπάνω, τα ιδιωτικά κλειδιά των χρηστών πρέπει να είναι ασφαλή, καθότι αν αυτά χαθούν, κλαπούν ή απλά αντιγραφούν, τότε η φερεγγυότητα της ανταλλαγής δεδομένων παύει να υφίσταται. Τέλος, ακόμα και με την κρυπτογραφία δημοσίου κλειδιού ο κίνδυνος πλαστοπροσωπίας είναι υπαρκτός. Τον κίνδυνο αυτό προσπαθεί να εξαλείψει η τριμερής ασύμμετρη κρυπτογραφία.

3.1.1.3. Η υπογραφή που στηρίζεται στην τριμερή ασύμμετρη κρυπτογραφία.

Για να είναι κάποιος απόλυτα βέβαιος ότι με τη χρήση ασύμμετρης κρυπτογραφίας δεν υπάρχει κίνδυνος υποκλοπής πρέπει εκ των προτέρων να γνωρίζει σε ποιον ανήκει ένα δημόσιο κλειδί. Σύμφωνα με τον, ο τρόπος για να επιτευχθεί αυτό είναι με την χρήση ενός έμπιστου τρίτου (trusted third party).[66]

Ο ρόλος αυτού του έμπιστου τρίτου είναι να μπορεί να εγγυηθεί και να πιστοποιήσει ότι τα δημόσια κλειδιά που χρησιμοποιούνται στην επικοινωνία ανάμεσα σε δύο αντισυμβαλλόμενα μέρη ανήκουν όντως στα μέρη αυτά. Ο «έμπιστος τρίτος» είναι υπεύθυνος για την επιβεβαίωση ότι ορισμένο δημόσιο κλειδί αντιστοιχεί στα απόρρητα στοιχεία που κωδικοποιούνται με το ιδιωτικό κλειδί κάποιου. Βασική δε προϋπόθεση στην τριμερή ασύμμετρη κρυπτογραφία είναι

[66] Choudhury, S , ό.π., σ. 30

τα αντισυμβαλλόμενα μέρη να γνωρίζουν εκ των προτέρων τον έμπιστο τρίτο και να αποδέχονται την «αυθεντία» του. Ειδικότερα, αυτός χορηγεί ηλεκτρονικά πιστοποιητικά, (ηλεκτρονικά αρχεία δηλαδή), τα οποία βεβαιώνουν την αντιστοιχία μεταξύ ιδιωτικού και δημόσιου κλειδιού, καθώς και ότι η τελευταία φέρει όλα τα εχέγγυα που απαιτούνται για τις ασφαλείς συναλλαγές.[67]

3.1.2. Οι έμπιστες τρίτες οντότητες και οι υπηρεσίες εμπιστοσύνης στις ηλεκτρονικές υπογραφές.

Ιδιαίτερος λόγος θα πρέπει να γίνει για τις έμπιστες τρίτες οντότητες και για τη λειτουργία που αυτές επιτελούν στην περίπτωση της ασύμμετρης κρυπτογραφικής μεθόδου για τις ηλεκτρονικές υπογραφές. Ειδικότερα, στο αχανές διαδίκτυο, όπου δεν μπορεί κάποιος να εγγυηθεί για την ασφάλεια των δεδομένων, τη σύνδεση του αποστολέα-κατόχου του ιδιωτικού κλειδιού, καθώς και την αξιόπιστη λειτουργία-αντιστοίχηση του δημοσίου την επιτελούν αυτές οι έμπιστες τρίτες οντότητες.

Με την ήδη (καταργηθείσα) Οδηγία 99/93/Ε.Κ., ως τέτοιος έμπιστος τρίτος περιγραφόταν ο «Πάροχος Υπηρεσιών Πιστοποίησης» (εφεξής ΠΥΠ). Ο δε ισχύων Κανονισμός (Ε.Ε.) 910/2014 διατήρησε την έννοια και τη λειτουργία του των παρόχων, («πάροχοι υπηρεσιών εμπιστοσύνης» διευρύνοντας τις παρεχόμενες υπηρεσίες και μετονόμαζοντές τις σε υπηρεσίες εμπιστοσύνης. Ειδικότερα, βάσει του Κανονισμού ως τέτοιος έμπιστος τρίτος-πάροχος υπηρεσιών εμπιστοσύνης θεωρείται το φυσικό ή νομικό πρόσωπο που παρέχει μία ή περισσότερες υπηρεσίες εμπιστοσύνης». (άρθρο 3 στοιχ. 19). Ως υπηρεσίες εμπιστοσύνης δε, ο ίδιος ο κανονισμός (άρθρο 3 στοιχ. 16) ορίζει την «ηλεκτρονική υπηρεσία, συνήθως παρεχόμενη έναντι αμοιβής, η οποία συνίσταται: α) στη δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων ή ηλεκτρονικών χρονοσφραγίδων, ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές, ή β) στη δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστοτόπων, ή γ) στη διαφύλαξη ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές». Τα προαναφερθέντα πιστοποιητικά[68] αφορούν στην ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης ηλεκτρονικής υπογραφής με φυσικό πρόσωπο και επιβεβαιώνει τουλάχιστον το όνομα ή το ψευδώνυμο του εν λόγω προσώπου (η έννοια των πιστοποιητικών εκτενώς αναλύεται στη συνέχεια της εργασίας). Συνεπώς, η ταυτοποίηση αυτού που υπογράφει το ηλεκτρονικό μήνυμα με αυτόν που είναι νόμιμος κάτοχος του δημοσίου κλειδιού αποκρυπτογράφησης του μηνύματος γίνεται μέσω του δημοσίου κλειδιού του ΠΥΠ. Έτσι, από

[67] Κορνηλία Δελούκα-Ιγγλέση, ό.π. , σ. 196 και Α. Μητρακά, ό.π., σ. 111
[68] Όπως αναφέρονται στο άρθρο 3 στοιχ. 14 του Κανονισμού (Ε.Ε.) 910/2014

τη μία πιστοποιείται η μοναδική σχέση του δημοσίου κλειδιού με τον ιδιοκτήτη του, ενώ ταυτόχρονα παρέχονται τα εχέγγυα ότι τα απόρρητα στοιχεία του του κατόχου του ιδιωτικού κλειδιού παραμένουν ασφαλή και η αποφεύγεται το ενδεχόμενο εξαπάτησης, που ελλόχευε στην περίπτωση της σύμμετρης κρυπτογράφησης.

3.1.3. Η ψηφιακή Υπογραφή

Καίτοι εσφαλμένα συχνά επικρατεί σύγχυση ανάμεσα στην έννοια της ηλεκτρονικής υπογραφής και της ψηφιακής υπογραφής, θα πρέπει να σημειωθεί ότι πρόκειται για έννοιες διακριτές μεταξύ τους. Ειδικότερα, όπως έχει επισημανθεί[69], η ηλεκτρονική υπογραφή αποτελεί πρωτίστως νομική έννοια, όπως αυτή αναλύθηκε ήδη.[70] Ο δε όρος της ψηφιακής υπογραφής χρησιμοποιείται για να περιγράψει μόνο την κατηγορία των ηλεκτρονικών υπογραφών οι οποίες δημιουργούνται με τη μέθοδο της (ασύμμετρης τριμερούς) κρυπτογραφίας. [71]Από άποψη, επομένως, μεθόδου δημιουργίας των ηλεκτρονικών υπογραφών συνάγεται ότι πρόκειται για την πλέον ασφαλή μέθοδο διαπίστωσης της ταυτότητας του «ηλεκτρονικώς υπογράφοντος», ενώ ταυτόχρονα εξασφαλίζεται όχι μόνο η εμπιστευτικότητα του αρχείου, αλλά και η ακεραιότητά του. Μάλιστα, όπως έχει τονιστεί «η ψηφιακή υπογραφή μας επιτρέπει να υπογράφουμε ένα μήνυμα με σκοπό να μπορούν να εντοπιστούν τυχόν αλλαγές στο περιεχόμενο του μηνύματος και να διασφαλίσουμε ότι ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του μηνύματος».[72]

Η διαδικασία δημιουργίας μίας ψηφιακής υπογραφής με τριμερή ασύμμετρη κρυπτογραφική μέθοδο από την πλευρά του αποστολέα περιλαμβάνει τα παρακάτω βήματα:

1. Ο αποστολέας δημιουργεί το αρχικό αρχείο που θέλει να αποστείλει.
2. Εκτελώντας έναν αλγόριθμο hash, δημιουργεί από το αρχικό αρχείο το hashed αρχείο.
3. Κωδικοποιεί το hashed αρχείο με τη χρήση του ιδιωτικού κλειδιού του.
4. Προσθέτει στο αρχικό αρχείο το κωδικοποιημένο hashed αρχείο.
5. Κωδικοποιεί το νέο αρχείο που προέκυψε από το βήμα 4 με τη χρήση του δημοσίου κλειδιού του παραλήπτη, το οποίο έχει επαληθεύσει μέσω του ΠΥΠ.
6. Αποστέλλει το αρχείο στον παραλήπτη.

[69] Κορνηλία Δελούκα-Ιγγλέση, υπ. σ. 183 επ.
[70] Βλ. Κεφάλαιο 2, ενότητες 2.2.-2.3. της παρούσης
[71] Χ. Μιχαηλίδου ό.π.
[72] Andress J. ό.π. σ. 80

Από τη μεριά του ο παραλήπτης, για να πιστοποιήσει την ψηφιακή υπογραφή, πρέπει να ακολουθήσει τα παρακάτω βήματα:

1. Αποκωδικοποίηση του αρχείου που παρέλαβε με το ιδιωτικό κλειδί του. Το αποκωδικοποιημένο αυτό αρχείο θα περιλαμβάνει το αρχικό κείμενο σε αναγνώσιμη μορφή καθώς και το κωδικοποιημένο hashed αρχείο.

2. Αποκωδικοποίηση του hashed αρχείου με το δημόσιο κλειδί του αποστολέα το οποίο επαληθεύει μέσω του ΠΥΠ.

3. Εκτέλεση του ίδιου αλγόριθμου hash στο αρχικό αρχείο. Αν το παραγόμενο hashed αρχείο συμπίπτει με το αποκρυπτογραφημένο hashed αρχείο τότε βεβαιώνεται η εγκυρότητα της ψηφιακής υπογραφής καθώς και του απεσταλμένου αρχείου.

Θα πρέπει να σημειωθεί δε, ότι υπό τις προϋποθέσεις που περιγράφει ο Κανονισμός (Ε.Ε.) 910/2014 (άρθρο 3 στοιχ. 11 – προηγμένες ηλεκτρονικές υπογραφές) η ψηφιακή υπογραφή μπορεί – τεχνολογικά – να επιτελέσει όλες τις επιθυμητές λειτουργίες των ηλεκτρονικών υπογραφών, ήτοι να εξασφαλίσει την αυθεντικότητα της επικοινωνίας, την ακεραιότητα των δεδομένων, καθώς και την προέλευσή τους. Μάλιστα, όταν πληρούνται τα επιπλέον κριτήρια του Κανονισμού για την εγκεκριμένη ηλεκτρονική υπογραφή, όπως αναλύεται κατωτέρω, η κρυπτογραφική αυτή μέθοδος αξιοποιείται για τη δημιουργία ηλεκτρονικής υπογραφής, η οποία εξομοιώνεται με την ιδιόχειρη υπογραφή.

3.2. Τα είδη της ηλεκτρονικής υπογραφής με κριτήριο τις διατάξεις του Κανονισμού 910/2014

Ήδη εξετάστηκε η μορφή των (απόρρητων) δεδομένων και η μέθοδος σύναψής τους σε άλλα ηλεκτρονικά δεδομένα (ηλεκτρονικά έγγραφα), ώστε να επιτευχθεί η τεκμηρίωση της γνησιότητας και της ακρίβειας της δήλωσης βουλήσεως του αποστολέα, καθώς και τα στοιχεία της ταυτότητας του . Ωστόσο, ήδη με τη την Οδηγία 99/93/Ε.Κ., όπως αυτή ενσωματώθηκε στο ελληνικό δίκαιο με το π.δ. 150/2001, παρατηρήθηκαν τρεις διαφορετικές περιπτώσεις-κατηγορίες ηλεκτρονικών υπογραφών, οι οποίες αναλύονται: σε απλές, προηγμένες και αναγνωρισμένες. Ακόμα όμως και με τη θέση σε ισχύ του Κανονισμού 910/2014, ήδη από το τρίτο άρθρο που παρατίθενται οι ορισμοί του νομοθετήματος, απαντά κανείς τρεις ορισμούς για την έννοια της ηλεκτρονικής υπογραφής. Αρχικά, ορίζεται η ηλεκτρονική υπογραφή,[73] εν συνεχεία η «προηγμένη ηλεκτρονική υπογραφή[74] και τέλος η «εγκεκριμένη ηλεκτρονική υπογραφή»[75]. Η ύπαρξη τριών κατηγοριών για τον προσδιορισμό της ίδιας νομικής έννοιας

[73] άρθρο 3 παρ. 10 του Κανονισμού (Ε.Ε.) αρ. 910/2014
[74] άρθρο 3 παρ. 11 του Κανονισμού (Ε.Ε.) αρ. 910/2014
[75] άρθρο3 παρ. 23 του Κανονισμού (Ε.Ε.) αρ. 910/2014

(ηλεκτρονική υπογραφή) προκαλεί εύλογα ερωτηματικά για το λόγο της ύπαρξής και αξιοποίησής τους από το σύγχρονο νομικό.

Όπως έχει επισημανθεί[76], προκειμένου να διασφαλιστεί ένα «υψηλό επίπεδο της αξιοπιστίας» των υπογραφών, ο Ευρωπαίος νομοθέτης ex lege έθεσε μόνον μία ορισμένη κατηγορία ηλεκτρονικής υπογραφής ως ισοδύναμη της (συμβατής) ιδιόχειρης (πλέον εγκεκριμένες ηλεκτρονικές υπογραφές). Ταυτόχρονα όμως ενόψει της αρχής της «τεχνολογικής ουδετερότητας» στην «ενιαία αγορά» η ίδια η Ευρωπαϊκή Κοινότητα (νυν Ευρωπαϊκή Ένωση) δεν ήταν δυνατό να απορρίψει κάθε άλλη πρόσφορη μέθοδο ηλεκτρονικής υπογραφής, εφόσον αυτή μπορούσε να είναι αξιόπιστη, ακόμα και εάν εξέλειπε κάποια από τις πολλαπλές απαιτούμενες προϋποθέσεις. Εκ των ανωτέρω λοιπόν, παρατηρείται μια διπλής διαβάθμισης προσέγγιση (two tier approach)[77] της ηλεκτρονικής υπογραφής.

Ήδη από τη θέσπιση της Οδηγία 99/93/Ε.Κ. μέχρι και σήμερα κατά την προσέγγιση της φύσης των ηλεκτρονικών υπογραφών ετέθησαν υψηλά ποιοτικά κριτήρια κατά τον προσδιορισμό της μορφής που θα έχει η ηλεκτρονική υπογραφή, ώστε να θεωρείται ισάξια της (συμβατής) ιδιόχειρης. Ωστόσο, προκειμένου να διαφυλαχτεί ακριβώς η βούληση των μερών-συμβαλλομένων, τα οποία για οποιοδήποτε λόγο δεν μπορούσαν να ανταποκριθούν στις πρόσθετες απαιτήσεις του Κανονισμού, έγινε (από)δεκτό να επαρκούν και εκείνα τα συνημμένα δεδομένα, τα οποία κατά την κρίση των εθνικών δικαστηρίων αρκούν για την απόδειξη της γνησιότητας των εξεταζόμενων κάθε φορά ηλεκτρονικών-ψηφιακών στοιχείων.

Για λόγους σκοπιμότητας εν προκειμένω, η εξέταση των τριών ειδών των υπογραφών θα ξεκινήσει από τις προηγμένες ηλεκτρονικές υπογραφές, θα συνεχιστεί με τις εγκεκριμένες ηλεκτρονικές υπογραφές και τέλος θα γίνει αναφορά στις απλές, οι οποίες παρέχουν και τις λιγότερες εγγυήσεις.

3.2.1. Οι προηγμένες ηλεκτρονικές υπογραφές

Στον Κανονισμό 910/2014 ο ορισμός της προηγμένης ηλεκτρονικής υπογραφής προκύπτει από το συνδυασμό των άρθρων 3 (παράγραφο 11) και του άρθρου 26. Ειδικότερα, πρόκειται για ηλεκτρονική υπογραφή (δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει), η οποία όμως ταυτόχρονα ικανοποιεί τις απαιτήσεις του άρθρου 26 του Κανονισμού. Ειδικότερα η προηγμένη ηλεκτρονική υπογραφή[78]:

[76] Βλ. αντί άλλων Σιούλης Χ., ό.π., σ. 2
[77] Στη ξένη και διεθνή βιβλιογραφία απαντάται και ως double tier approach
[78] Κοσμάς Α. Καραδημητρίου, ό.π., σ. 121-122

α) συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα, ήτοι τα συνημμένα δεδομένα αφορούν αποκλειστικά και μόνο τον υπογράφοντα. Πρόκειται για την κατοχή ιδιωτικού κλειδιού και των απόρρητων πληροφοριών που αυτό ενσωματώνει κατά τις προαναφερθείσες μεθόδους κρυπτογραφίας.

β) είναι ικανή να ταυτοποιεί τον υπογράφοντα. Πληροί δηλαδή τα κριτήρια της διαδικασίας τεκμηρίωσης και μπορεί να επιβεβαιωθεί ο αποστολέας του (κρυπτογραφημένου) μηνύματος ως το πρόσωπο που υπέγραψε.

γ) δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής, τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο. Πρόκειται δηλαδή για τα μοναδικά δεδομένα που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής (άρθρο 3 παρ. 13 του Κανονισμού). Όπως αναφέρθηκε, τα δεδομένα αυτά αφορούν στο ιδιωτικό κλειδί κατά τη δημιουργία ηλεκτρονικής υπογραφής με κρυπτογραφικές μεθόδους, το οποίο (ιδιωτικό κλειδί) ο υπογράφων θα πρέπει να το ελέγχει απόλυτα και να αποκλείει την τυχόν παρέμβαση ή αξιοποίησή του από τρίτους.

δ) συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτήν κατά τρόπο που να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.

Προκειμένου να γίνει αντιληπτή η σημασία των προηγμένων ηλεκτρονικών υπογραφών θα πρέπει εδώ να αναφέρουμε τη σημασία τους κατά το προϊσχύσαν δίκαιο. Ο ορισμός της προηγμένης ηλεκτρονικής υπογραφής κατά την Οδηγία 99/93/Ε.Κ.[79] αφορούσε «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα, με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (ορισμός ηλεκτρονικής υπογραφής κατά την Οδηγία 99/93/Ε.Κ.), ενώ ταυτόχρονα για να είναι προηγμένη αυτή θα έπρεπε «α) να συνδέεται μονοσήμαντα με τον υπογράφοντα· β) είναι ικανή να ταυτοποιήσει τον υπογράφοντα· γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων.». Τον ίδιο βέβαια ορισμό υιοθέτησε και ο Έλληνας νομοθέτης με το άρθρο 2 παρ. 2 του π.δ. 150/2001. Έχει δε επισημανθεί[80], ότι η συγκεκριμένη περίπτωση «φωτογραφίζει» τη δημιουργία ηλεκτρονικής υπογραφής με τη μέθοδο της ασύμμετρης κρυπτογραφίας, με όλα τα εχέγγυα που αυτή παρέχει (πόσο μάλλον στην περίπτωση που αυτή είναι τριμερής). Αυτό άλλωστε στηρίζεται και στην δεύτερη απαίτηση για τις προηγμένες ηλεκτρονικές υπογραφές (ταυτοποίηση του υπογράφοντα), αφού με την ύπαρξη δημόσιου

[79] άρθρο 2 παρ. 2 της Οδηγίας 99/93Ε.Κ.
[80] Κορνηλία Δελούκα Ιγγλέση, ό.π. σ. 205

κλειδιού, όχι μόνο αυτή επιτυγχάνεται με τρόπο βέβαιο, αλλά πολύ περισσότερο διασφαλίζεται και η ασφάλεια του ιδιωτικού κλειδιού.[81]

Επιπλέον, αποτέλεσε κοινό τόπο στη νομική θεωρία ήδη κατά το προϊσχύσαν δίκαιο ότι ο ορισμός των προηγμένων ηλεκτρονικών υπογραφών, έδωσε έμφαση στις λειτουργίες που αυτή επιτελεί και όχι στην τεχνολογία που αξιοποιείται, αφήνοντας έτσι μεγάλο περιθώριο ευελιξίας και προσαρμοστικότητας στις αξιοποιούμενες μεθόδους της ταχέως εξελισσόμενης ψηφιακής εποχής. Έτσι βέβαια και ο νέος Κανονισμός (Ε.Ε.) 910/2014, αναγνώρισε (σκέψη 50 Προοιμίου) ότι τα κράτη μέλη χρησιμοποιούσαν διαφορετικές μορφές προηγμένων ηλεκτρονικών υπογραφών. Ωστόσο προκειμένου να ενισχυθεί η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές εντός της εσωτερικής αγοράς, αναγνωρίζεται πλέον ως επιτακτική η ανάγκη εξασφάλισης ενός αριθμού προηγμένων ηλεκτρονικών υπογραφών (προτύπων) που θα μπορεί να υποστηρίζεται από όλα τα κράτη μέλη, όταν λαμβάνουν έγγραφα με ηλεκτρονική υπογραφή.

3.2.2. Οι εγκεκριμένες ηλεκτρονικές υπογραφές

Η έννοια των εγκεκριμένων ηλεκτρονικών υπογραφών του Κανονισμού 910/2014 (άρθρο 3 παρ. 12) ήρθε να αντικαταστήσει την έννοια των «αναγνωρισμένων ηλεκτρονικών υπογραφών»[82], όπως εμμέσως αναγνωρίζονταν από το άρθρο 5 παρ. 1 της Οδηγίας 99/93ΕΚ και στο άρθρο 3 παρ. 1 του π.δ. 150/2001. Ειδικότερα, επρόκειτο για «προηγμένες ηλεκτρονικές υπογραφές» για τις οποίες απαιτείτο υποστήριξή τους από «αναγνωρισμένο πιστοποιητικό», αλλά και η «χρήση ασφαλούς διάταξης δημιουργίας ηλεκτρονικής υπογραφής». Οι επιπλέον αυτές απαιτήσεις εξασφάλιζαν «το μεγαλύτερο δυνατό βαθμό πιθανολογικής ασφάλειας ως προς την προέλευση και ως προς το αναλλοίωτο του ηλεκτρονικού εγγράφου», με αποτέλεσμα να αναγνωρίζονται ισότιμες με τις (συμβατές) ιδιόχειρες ηλεκτρονικές υπογραφές.[83]

Αντίστοιχα στον Κανονισμό ως εγκεκριμένη ηλεκτρονική υπογραφή ορίζεται η «προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής και η οποία βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής» (άρθρο 3 παρ. 12 του Κανονισμού). Συνεπώς, εν προκειμένω ισχύουν όλα όσα ανωτέρω αναφέρθηκαν για τις προηγμένες ηλεκτρονικές υπογραφές, ενώ τονίζεται ότι και αυτή η κατηγορία βασίζεται στη μέθοδο της τριμερούς ασύμμετρης κρυπτογραφίας.

[81] Αντί πολλών βλ. Χ. Μιχαηλίδου, ό.π., σ. 4
[82] Ι. Ιγγλεζάκη, ό.π., σ. 220επ.
[83] Κορνηλία Δελούκα-Ιγγλέση, ό.π. σ. 206

Ο ενωσιακός νομοθέτης έκρινε σκόπιμο να ορίσει ευθέως για τις εγκεκριμένες ηλεκτρονικές υπογραφές, ότι έχουν νομική ισχύ ισοδύναμη των ιδιόχειρων υπογραφών και ότι αναγνωρίζονται σε όλα τα κράτη μέλη της Ένωσης[84], πληρουμένων των δύο απαιτήσεων που αναφέρονται στον ανωτέρω ορισμό. Ειδικότερα, οι εγκεκριμένες ηλεκτρονικές υπογραφές, υπό τις προαναφερθείσες προϋποθέσεις, καθιστούν το ηλεκτρονικό έγγραφο δεσμευτικό, ως να είχε υπογραφεί ιδιοχείρως, επιφέροντας έτσι όλες τις έννομες συνέπειες σε ζητήματα ουσιστικού και δικονομικού δικαίου.[85]

Ο Κανονισμός (Ε.Ε.) 910/2014 αφιερώνει το τέταρτο μέρος (άρθρα 25 – 34) για να αναφερθεί σε τεχνολογίες απαραίτητες για τη δημιουργία των εγκεκριμένων ηλεκτρονικών υπηρεσιών σχετιζόμενων με αυτές, καθώς και τους φορείς που τις επιτελούν. Όλα τα ανωτέρω αναλύονται αμέσως κατωτέρω, αρχής γενομένης από τις εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής και των εγκεκριμένων πιστοποιητικών, που αποτελούν απαραίτητη προϋπόθεση δημιουργίας της υπό εξέταση κατηγορίας εγγραφών.

3.2.2.1. Οι εγκεκριμένες διατάξεις δημιουργία ηλεκτρονικής υπογραφής

Οι εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής αφορούν εκείνο το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για τη δημιουργία ηλεκτρονικής υπογραφής (διατάξεις δημιουργίας ηλεκτρονικής υπογραφής – άρθρο 3 παρ. 22), το οποίο όμως πληροί τις προϋποθέσεις του Κανονισμού, ώστε αξιοποιούμενων[86] των κατάλληλων τεχνικών και διαδικαστικών μέσων να πληρούνται οι ελάχιστες προϋποθέσεις του κανονισμού, όπως αυτές αναφέρονται στο Παράρτημα ΙΙ του Κανονισμού (Ε.Ε.) 910/2014.

Τονίζεται δε ότι οι εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής δεν θα πρέπει να μεταβάλλουν τα προς υπογραφή δεδομένα, ούτε να εμποδίζουν την υποβολή τους στον υπογράφοντα πριν από την υπογραφή. Μάλιστα, τόσο η δημιουργία, όσο και η διαχείριση των δεδομένων δημιουργίας των υπογραφών εκ μέρους του υπογράφοντος, μπορεί να πραγματοποιείται μόνο από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης. Με αυτό τον τρόπο επιτυγχάνεται η αξιοπιστία και η μυστικότητα κατά τη δημιουργία της εγκεκριμένης ηλεκτρονικής υπογραφής.

Τέλος σημειώνεται ότι οι ηλεκτρονικές υπογραφές θα πρέπει να παράγονται με μέσα, σύμφωνα με τα οποία:

[84] Βλ. άρθρο 25 παρ. 2-3 του Κανονισμού (Ε.Ε.) 910/2014
[85] Μητρακάς Α., όπ, σ. 109-111
[86] Βλ. άρθρο 3 παρ.23 του Κανονισμού (Ε.Ε.) 910/2014

α) διασφαλίζεται ευλόγως η εμπιστευτικότητα των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία της ηλεκτρονικής υπογραφής·

β) τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία της ηλεκτρονικής υπογραφής μπορούν να προκύψουν στην πράξη μία μόνο φορά·

γ) τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία ηλεκτρονικής υπογραφής δεν μπορούν με εύλογη βεβαιότητα να είναι παράγωγα και ότι η ηλεκτρονική υπογραφή προστατεύεται με τρόπο αξιόπιστο από πλαστογραφία με τη χρήση της τρέχουσας τεχνολογίας·

δ) τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία ηλεκτρονικής υπογραφής μπορούν να προστατεύονται κατά τρόπο αξιόπιστο από τον νόμιμο υπογράφοντα έναντι της χρησιμοποίησης τους από τρίτους, πλην των περιπτώσεων που οι εγκεκριμένοι Πάροχοι Υπηρεσιών Πιστοποίησης κληθούν να αναπαράγουν τα δεδομένα αυτά μόνο για λόγους δημιουργίας εφεδρικών αντιγράφων. Ακόμα και σε αυτή την περίπτωση όμως, η χρήση των δεδομένων επιτρέπεται μόνο για την εξασφάλιση της συνέχισης της υπηρεσίας με την αναπαραγωγή τους και αυτό προκειμένου η ασφάλεια των αναπαραγόμενων δεδομένων να είναι στο ίδιο επίπεδο με αυτό της ασφάλειας των πρωτοτύπων.

3.2.2.2. Τα εγκεκριμένα πιστοποιητικά

Ως εγκεκριμένο Πιστοποιητικό στον Κανονισμό[87] είναι η ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης (της εγκεκριμένης) ηλεκτρονικής υπογραφής με φυσικό πρόσωπο και επιβεβαιώνει τουλάχιστον το όνομα ή το ψευδώνυμο του εν λόγω προσώπου και εκδίδεται μόνο από εποπτικό φορέα που έχει διαπιστευτεί και εποπτεύεται από αρχές[88] που ορίζονται από τα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Μάλιστα, όπως απαιτείται από τον Κανονισμό τα εγκεκριμένα πιστοποιητικά ηλεκτρονικής υπογραφής πρέπει να περιέχουν όλα τα ακόλουθα στοιχεία:

α) ένδειξη, τουλάχιστον σε μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία, ότι το πιστοποιητικό έχει εκδοθεί ως εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής·

β) ένα σύνολο δεδομένων που αντιπροσωπεύουν αναμφίσημα τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, ο οποίος έχει εκδώσει τα εγκεκριμένα πιστοποιητικά και περιλαμβάνουν τουλάχιστον το κράτος μέλος στο οποίο είναι εγκατεστημένος και α) σε

[87] Ως προκύπτει από το συνδυασμό των παραγράφων 14 και 15 του άρθρου 3 του Κανονισμού (Ε.Ε.) 910/2014

[88] Στην Ελλάδα πρόκειται για την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (βλ. κατωτέρω οικεία ανάλυση στην ενότητα 4.2.2.7. σ.49)

περίπτωση που πρόκειται για νομικό πρόσωπο: το όνομα και, κατά περίπτωση, τον αριθμό μητρώου του, όπως αναφέρεται στα επίσημα αρχεία, ενώ β) σε περίπτωση που πρόκειται για φυσικό πρόσωπο: το όνομα του προσώπου·

γ) τουλάχιστον το όνομα του υπογράφοντος ή ένα ψευδώνυμο· εάν χρησιμοποιείται ψευδώνυμο, πρέπει να αναφέρεται σαφώς·

δ) δεδομένα επικύρωσης ηλεκτρονικής υπογραφής, που αντιστοιχούν στα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής·

ε) λεπτομέρειες για την έναρξη και τη λήξη της περιόδου ισχύος του πιστοποιητικού·

στ) τον κωδικό ταυτότητας του πιστοποιητικού, ο οποίος πρέπει να είναι μοναδικός για τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης·

ζ) την προηγμένη ηλεκτρονική υπογραφή (…) του εκδίδοντος εγκεκριμένου παρόχου υπηρεσιών εμπιστοσύνης·

η) την τοποθεσία όπου διατίθεται δωρεάν το πιστοποιητικό το οποίο τεκμηριώνει την προηγμένη ηλεκτρονική υπογραφή (…)

θ) την τοποθεσία των υπηρεσιών που μπορούν να χρησιμοποιηθούν για την άντληση πληροφοριών σχετικά με το καθεστώς ισχύος του εγκεκριμένου πιστοποιητικού·

ι) σε περίπτωση που τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής, τα οποία σχετίζονται με τα δεδομένα επικύρωσης ηλεκτρονικής υπογραφής, βρίσκονται σε εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής, κατάλληλη σχετική ένδειξη, τουλάχιστον σε μορφή κατάλληλη για αυτοματοποιημένη επεξεργασία.

3.2.2.3. Οι υπηρεσίες διαφύλαξης εγκεκριμένων ηλεκτρονικών υπογραφών

Ήδη από το Προοίμιο του νέου Κανονισμού[89] αναγνωρίζεται η ανάγκη εξασφάλισης της μακροπρόθεσμης διαφύλαξης των πληροφοριών, ώστε να διασφαλίζεται η νομική εγκυρότητα της ηλεκτρονικής υπογραφής για μεγάλα χρονικά διαστήματα, ανεξάρτητα μελλοντικών τεχνολογικών αλλαγών.

Η διαφύλαξη των δεδομένων της ηλεκτρονικής υπογραφής εντάσσεται στις υπηρεσίες εμπιστοσύνης, στις οποίες ήδη έχουμε αναφερθεί. Ωστόσο, εν προκειμένω για τις εγκεκριμένες

[89] Χαρακτηριστικά στην αιτιολογική σκέψη 61 του Προοιμίου αναφέρεται: «Ο παρών κανονισμός θα πρέπει να εξασφαλίζει τη μακροπρόθεσμη διαφύλαξη των πληροφοριών για τη διασφάλιση της νομικής εγκυρότητας της ηλεκτρονικής υπογραφής και των ηλεκτρονικών σφραγίδων για μεγάλα χρονικά διαστήματα και για την εξασφάλιση πως θα μπορούν να επικυρωθούν ανεξάρτητα από τις μελλοντικές τεχνολογικές αλλαγές.»

ηλεκτρονικές υπογραφές, στον Κανονισμό (Ε.Ε.) 910/2014 με τρόπο σαφή ορίζεται[90], ότι στην περίπτωσή τους, πρόκειται για εγκεκριμένη υπηρεσία διαφύλαξης τους, η οποία μπορεί να παρέχεται μόνο από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, ο οποίος χρησιμοποιεί διαδικασίες και τεχνολογίες ικανές να επεκτείνουν την αξιοπιστία της εγκεκριμένης ηλεκτρονικής υπογραφής πέραν της περιόδου τεχνολογικής ισχύος. Μάλιστα, προκειμένου για τη διασφάλιση των υπηρεσιών αυτών η Επιτροπή μπορεί να καθορίζει τα πρότυπα αναφοράς, τα οποία, εφόσον ακολουθούνται θα τεκμαίρεται ότι η παροχή των εγκεκριμένων υπηρεσιών διαφύλαξης γίνεται αξιοποιούμενων των πλέον τελέσφορων τεχνολογικών μεθόδων.

Θα πρέπει να σημειωθεί εν προκειμένω, ότι τόσο για την υπό εξέταση εγκεκριμένη υπηρεσία, όσο και για την εγκεκριμένη υπηρεσία επικύρωσης (αμέσως κατωτέρω), ήδη εκ Προοιμίου (σκέψη 58) του Κανονισμού διαπιστώθηκε, ότι θα πρέπει να γίνεται με βάση πιστοποιημένες εγκεκριμένες διατάξεις. Όπως αναφέρεται δε στον Κανονισμό (άρθρο 30) αυτές πιστοποιούνται από αρμόδιους δημόσιους ή ιδιωτικούς φορείς. Αυτή δε θα πρέπει να βασίζεται είτε στη διαδικασία αξιολόγησης της ασφάλειας διενεργούμενη σύμφωνα με κάποιο από τα υπάρχοντα πρότυπα που περιλαμβάνονται σε κατάλογο τον οποίο καταρτίζει η Επιτροπή ή - υπό συγκεκριμένες περιστάσεις - σε διαδικασία διαφορετική, εφόσον όμως αυτή χρησιμοποιεί συγκρίσιμα επίπεδα ασφάλειας και γνωστοποιείται στην Επιτροπή. Μάλιστα, επ' αυτού δημοσιεύτηκε η εκτελεστική απόφαση (Ε.Ε.) 2016/650 της Επιτροπής, δια της οποίας ετέθησαν τα πρότυπα για την αξιολόγηση της ασφάλειας των προϊόντων πληροφορικής που εφαρμόζονται στην πιστοποίηση των εγκεκριμένων διατάξεων δημιουργίας ηλεκτρονικής υπογραφής.

3.2.2.4. Η εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών

Ήδη πριν τη θέση σε ισχύ του ισχύοντος Κανονισμού (Ε.Ε.) 910/2014 είχε καταστεί αντιληπτή η ανάγκη δημιουργίας μίας υποδομής δημόσιου κλειδιού σε πανευρωπαϊκό επίπεδο, για την ενίσχυση της ασφάλειας των ηλεκτρονικών υπηρεσιών και δη των ηλεκτρονικών υπογραφών στα πλαίσια της ολοκλήρωσης της εσωτερικής αγοράς για το ηλεκτρονικό εμπόριο. Στα ίδια πλαίσια κινούμενη η Ευρωπαϊκή Επιτροπή, κατά την υποβληθείσα πρόταση[91] για έναν κανονισμό σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά, υποστήριξε τη δυνατότητα επικύρωσης των

[90] άρθρο 34 του Κανονισμού (Ε.Ε.) 910/2014

[91] Ευρωπαϊκή Επιτροπή, Πρόταση: ΚΑΝΟΝΙΣΜΟΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά, COM(2012) 238 final, διαθέσιμο στην ηλεκτρονική διεύθυνση https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52012PC0238&from=EL, (ημερομηνία επίσκεψης 28-05-2020)

υπαρχουσών ηλεκτρονικών υπογραφών. Με αυτό τον τρόπο θα ενισχυόταν η διασυνοριακή διαλειτουργικότητα των ηλεκτρονικών υπογραφών .

Με τον Κανονισμό (Ε.Ε.) 910/2014 προβλέπεται η δυνατότητα εξέτασης της εγκυρότητας της υπογραφής, ώστε αυτή να μπορεί να αναγνωριστεί – επικυρωθεί υπό τις τιθέμενες προϋποθέσεις ως εγκεκριμένη ηλεκτρονική υπογραφή. Στην πράξη δηλαδή, εξετάζεται και αξιολογείται κατά πόσο πληρούνται τα απαραίτητα συστατικά στοιχεία της εγκεκριμένης ηλεκτρονικής υπογραφής. Ειδικότερα, στο άρθρο 33 του εν λόγω Κανονισμού προβλέπεται η παροχή της εγκεκριμένης υπηρεσίας επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών. Η εγκυρότητα δε, επιβεβαιώνεται εφόσον αυτή πραγματοποιείται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, ενώ θα πρέπει να διασφαλίζεται ότι το σύστημα που χρησιμοποιείται για την επικύρωση της ηλεκτρονικής υπογραφής παρέχει στο βασιζόμενο μέρος (το πρόσωπο που βασίζεται στην υπό εξέταση υπηρεσία εμπιστοσύνης) το ορθό αποτέλεσμα της διαδικασίας επικύρωσης και του επιτρέπει να εντοπίζει τυχόν ζητήματα ασφαλείας. Ταυτόχρονα δε, για τη διαδικασία της επικύρωσης θα πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις:

α) το πιστοποιητικό που τεκμηριώνει την υπογραφή, ήταν κατά τη στιγμή της υπογραφής εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής[92]·

β) το εγκεκριμένο πιστοποιητικό εκδόθηκε από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και ήταν έγκυρο κατά τη στιγμή της υπογραφής·

γ) τα στοιχεία επικύρωσης της υπογραφής αντιστοιχούν στα δεδομένα που παρέχονται στο βασιζόμενο μέρος·

δ) το μοναδικό σύνολο δεδομένων που αντιπροσωπεύουν τον υπογράφοντα στο πιστοποιητικό παρέχεται ορθώς στο βασιζόμενο μέρος·

ε) η χρήση οποιουδήποτε ψευδώνυμου δηλώνεται εμφανώς στο βασιζόμενο μέρος, εάν χρησιμοποιήθηκε ψευδώνυμο κατά τη στιγμή της υπογραφής·

στ) η ηλεκτρονική υπογραφή δημιουργήθηκε από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής·

ζ) η ακεραιότητα των υπογεγραμμένων δεδομένων δεν έχει τεθεί σε κίνδυνο·

η) κατά τη στιγμή της υπογραφής πληρούνταν οι απαιτήσεις που προβλέπονται στο άρθρο 26.

3.2.2.5. Οι εγκεκριμένες υπηρεσίες εμπιστοσύνης

[92] Βλ. ανωτέρω ενότητα 4.2.2.2. Τα εγκεκριμένα πιστοποιητικά, σ.

Ήδη έγινε λόγος για τις παρεχόμενες υπηρεσίες εμπιστοσύνης από τους «έμπιστους τρίτους» - παρόχους τους στα πλαίσια της μεθόδου δημιουργίας των ηλεκτρονικών υπογραφών βάσει της τριμερούς ασύμμετρης κρυπτογραφίας, στην οποία, όπως τονίστηκε, βασίζονται οι προηγμένες ηλεκτρονικές υπογραφές και κατ' επέκταση οι υπό εξέταση εγκεκριμένες. Στην παρούσα ενότητα, πρόκειται να εξεταστούν οι εγκεκριμένες υπηρεσίες εμπιστοσύνης, οι οποίες αφορούν την περίπτωση των εγκεκριμένων ηλεκτρονικών υπογραφών.

Ειδικότερα, ο ισχύων Κανονισμός (Ε.Ε.) 910/2014, καίτοι αναγνωρίζει τη δυνατότητα στο κάθε κράτος μέλος να ορίζει ελεύθερα τις υπηρεσίες εμπιστοσύνης, πέραν των αναφερόμενων στον κατάλογο του άρθρου 3, επισημαίνει ότι μόνο εκείνες που συνάδουν με τις περιεχόμενες σε αυτόν διατάξεις μπορούν να κυκλοφορούν ελεύθερα στην εσωτερική αγορά.[93] Ωστόσο, τονίζεται ότι για να ενισχυθεί κυρίως η εμπιστοσύνη των μικρομεσαίων επιχειρήσεων και των καταναλωτών στην εσωτερική αγορά και να προωθηθεί η χρήση των υπηρεσιών και των προϊόντων εμπιστοσύνης, θα πρέπει να εισαχθούν οι έννοιες των εγκεκριμένων υπηρεσιών εμπιστοσύνης και των εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης, με σκοπό να προσδιοριστούν οι απαιτήσεις και οι υποχρεώσεις που εξασφαλίζουν υψηλού επιπέδου ασφάλεια κατά τη χρήση ή την παροχή οιωνδήποτε εγκεκριμένων υπηρεσιών και προϊόντων εμπιστοσύνης.[94]

Όλα τα κράτη μέλη θα πρέπει να τηρούν κοινές βασικές απαιτήσεις εποπτείας, προκειμένου να διασφαλίζεται ένα συγκρίσιμο επίπεδο ασφάλειας για τις εγκεκριμένες υπηρεσίες εμπιστοσύνης. Προκειμένου να διευκολύνουν την ομοιόμορφη εφαρμογή αυτών των απαιτήσεων σε ολόκληρη την Ένωση, τα κράτη μέλη θα πρέπει να εγκρίνουν συγκρίσιμες διαδικασίες και να ανταλλάσσουν πληροφορίες σχετικά με τις εποπτικές δραστηριότητες και τις βέλτιστες πρακτικές τους στον τομέα αυτό. Εξ αυτής της προϋποθέσεως, η οποία τίθεται ήδη στο Προοίμιο του παρόντος Κανονισμού, συνάγεται ότι για τον προσδιορισμό των εγκεκριμένων υπηρεσιών συνιστώνται οι διαδικασίες που ακολουθούνται κατά την παροχή των εγκεκριμένων υπηρεσιών. Ειδικότερα, όπως επισημάνθηκε κατά τις ανωτέρω εκτεθείσες εγκεκριμένες υπηρεσίες, τα κριτήρια μπορούν να αφορούν στην υποχρέωση να ακολουθείται

[93] Βλ. και αιτιολογική σκέψη 27 του Προοιμίου του Κανονισμού 910/2014: «Ο παρών κανονισμός θα πρέπει να είναι τεχνολογικά ουδέτερος. Η νομική ισχύς που παρέχει θα πρέπει να μπορεί να επιτευχθεί με οιοδήποτε τεχνικό μέσο υπό την προϋπόθεση ότι πληρούνται οι απαιτήσεις του παρόντος κανονισμού.»

[94] Βλ. αιτιολογική σκέψη 28 του Προοιμίου του Κανονισμού 910/2014: «Για να ενισχυθεί κυρίως η εμπιστοσύνη των μικρομεσαίων επιχειρήσεων (ΜΜΕ) και των καταναλωτών στην εσωτερική αγορά και να προωθηθεί η χρήση των υπηρεσιών και των προϊόντων εμπιστοσύνης, θα πρέπει να εισαχθούν οι έννοιες των εγκεκριμένων υπηρεσιών εμπιστοσύνης και των εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης, με σκοπό να προσδιοριστούν οι απαιτήσεις και οι υποχρεώσεις που εξασφαλίζουν υψηλού επιπέδου ασφάλεια κατά τη χρήση ή την παροχή οιωνδήποτε εγκεκριμένων υπηρεσιών και προϊόντων εμπιστοσύνης.»

συγκεκριμένη διαδικασία, να παρέχονται συγκεκριμένες δυνατότητες ή/και να απαιτούνται συγκεκριμένα τεχνολογικά μέσα.

Μάλιστα, προκειμένου οι χρήστες να αξιοποιούν πλήρως και να στηρίζονται συνειδητά στις ηλεκτρονικές υπηρεσίες είναι απαραίτητο να υπάρχει εμπιστοσύνη στις επιγραμμικές υπηρεσίες και να διασφαλίζεται η ευχρηστία τους. Για τον σκοπό αυτό, στο άρθρο 23 παρ. 3 προβλέπεται η δημιουργία ενωσιακού σήματος εμπιστοσύνης, που θα επισημαίνει τις εγκεκριμένες υπηρεσίες εμπιστοσύνης που παρέχονται από εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης. Οι προδιαγραφές αυτού του σήματος προσδιορίζονται στον Εκτελεστικό Κανονισμό (Ε.Ε.) 2015/806 της Επιτροπής.

Σε επίπεδο του κάθε κράτους μέλους επιφορτισμένη με τον προσδιορισμό των εγκεκριμένων διαδικασιών είναι η εκάστοτε αρμόδια εποπτική αρχή. Στην περίπτωση της Ελλάδας, πρόκειται για την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ). Η τελευταία ανταποκρίθηκε στην υποχρέωση να κοινοποιήσει τις εγκεκριμένες υπηρεσίες, οι οποίες όχι μόνο αναγνωρίζονται στην περίπτωση της Ελλάδας, αλλά και στα υπόλοιπα κράτη μέλη της Ένωσης. Ειδικότερα, όπως αναφέρεται στο Παράρτημα Ι του Κανονισμού Παροχής Υπηρεσιών Εμπιστοσύνης[95] οι αναγνωρισμένες στην Ελλάδα παρεχόμενες εγκεκριμένες υπηρεσίες είναι οι κάτωθι:

1. Δημιουργία εγκεκριμένης Ηλεκτρονικής Υπογραφής

2. Δημιουργία εγκεκριμένης Ηλεκτρονικής Σφραγίδας

3. Επικύρωση εγκεκριμένης Ηλεκτρονικής Υπογραφής

4. Επικύρωση εγκεκριμένης Ηλεκτρονικής Σφραγίδας

5. Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Υπογραφής

6. Διαφύλαξη εγκεκριμένης Ηλεκτρονικής Σφραγίδας

7. Δημιουργία εγκεκριμένης Ηλεκτρονικής Χρονοσφραγίδας

8. Υπηρεσία Συστημένης Παράδοσης

9. Δημιουργία εγκεκριμένων πιστοποιητικών Γνησιότητας Ιστοτόπων

3.2.2.6. Οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης

Οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης και η αναλυτική προσέγγιση του ισχύοντος Κανονισμού είναι ιδιαίτερης σημασίας. Αρχικά, έχει γίνει ήδη αντιληπτό από τη μέχρι τώρα

[95] Η υπ' αρ. 837/1Β απόφαση, ΦΕΚ Β 4396/14-12-2017

ανάλυση ότι η οποιαδήποτε εγκεκριμένη υπηρεσία παράγεται αποκλειστικά από εγκεκριμένους παρόχους. Εύλογα λοιπόν δημιουργείται η απορία ποιες οντότητες περιλαμβάνονται σε αυτή την περίπτωση.

Ο Κανονισμός (Ε.Ε.) 910/2014 στο άρθρο 3 παρ. 19-20 ορίζει ως εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης το φυσικό ή νομικό πρόσωπο που παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει αναγνωριστεί ως τέτοιο από τον εποπτικό φορέα. Ειδικότερα η διαδικασία έναρξης παροχής εγκεκριμένων υπηρεσιών περιγράφεται στο άρθρο 21 του Κανονισμού. Ο υποψήφιος πάροχος υποβάλει στον εποπτικό φορέα, όχι μόνο την πρόθεση έναρξης παροχής εγκεκριμένων υπηρεσιών εμπιστοσύνης, αλλά και έκθεση αιτιολόγησης, η οποία καταδεικνύει τη συμμόρφωσή του προς τις απαιτούμενες διαδικασίες των εγκεκριμένων διαδικασιών. Εφόσον, η εποπτεύουσα αρχή-αρμόδιος φορέας διαπιστώσει ότι τόσο ο υποψήφιος φορέας, όσο και οι υπηρεσίες που πρόκειται να παρέχονται ως εγκεκριμένες συμμορφώνονται στις απαιτήσεις του Κανονισμού, εγκρίνει την αίτηση αυτή και συμπεριλαμβάνει τον πάροχο στον Κατάλογο Εμπίστευσης εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης (Trusted List). Από εκείνη τη στιγμή, ο πάροχος υπηρεσιών εμπιστοσύνης κρίνεται ως εγκεκριμένος. Μάλιστα, θα πρέπει να σημειωθεί ότι σε ετήσια βάση ο εν λόγω Πάροχος υπόκειται σε έλεγχο συμμόρφωσης από τον αρμόδιο οργανισμό αξιολόγησης, προκειμένου να επιβεβαιώνεται ότι οι παρεχόμενες από τους ελεγχόμενους φορείς εγκεκριμένες υπηρεσίες εμπιστοσύνης πληρούν τις απαιτήσεις του παρόντος Κανονισμού. Στην περίπτωση της Ελλάδας, όπως έχει τονιστεί αρμόδιος φορέας για την έγκριση των εγκεκριμένων παρόχων υπηρεσιών είναι η ΕΕΤΤ, δυνάμει του άρθρου 48 του νόμου 4487/2017. Η δε διαδικασία έγκρισης των εγκεκριμένων παρόχων περιγράφεται στον Κανονισμό Παροχής Υπηρεσιών Εμπιστοσύνης (υπ' αρ. 837/1Β απόφαση, ΦΕΚ Β 4396/14-12-2017).

Ήδη όμως με τον Κανονισμό προβλέπονται αυξημένες ευθύνες των εγκεκριμένων Παρόχων. Και τούτο φαίνεται εύλογο δεδομένου του ρόλου που επιτελούν**.** Έτσι, ήδη στο προοίμιο του Κανονισμού[96] διευκρινίζεται ότι οι εν γένει Πάροχοι υπηρεσιών εμπιστοσύνης καθίστανται υπεύθυνοι για την ασφάλεια και την ευθύνη, τη διασφάλιση της δέουσας επιμέλειας, της διαφάνειας και της λογοδοσίας των δραστηριοτήτων και των υπηρεσιών τους. Ωστόσο, η ευθύνη των εγκεκριμένων παρόχων είναι σαφώς βαρύτερη, αφού σε ό,τι αφορά τις περιπτώσεις των μη εγκεκριμένων Παρόχων η εποπτεία είναι αρκετά πιο χαλαρή[97].

[96] Βλ. αιτιολογική σκέψη 35 του Κανονισμού (Ε.Ε.) 910/2014

[97] Βλ. αιτιολογική σκέψη 36 του Κανονισμού (Ε.Ε.) 910/2014: «(…)Οι μη εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να υπόκεινται σε ήπιες και αντενεργές εκ των υστέρων εποπτικές δραστηριότητες, δικαιολογούμενες από τη φύση των υπηρεσιών και των πράξεων.»

Ειδικότερα, στο άρθρο 13 του Κανονισμού η ευθύνη των παρόχων (εγκεκριμένων ή μη) συνίσταται σε αποκατάσταση κάθε ζημίας που προκαλείται από πρόθεση ή από αμέλεια σε οποιοδήποτε φυσικό ή νομικό πρόσωπο, λόγω μιας μη συμμόρφωσης προς τις υποχρεώσεις που προβλέπονται στον παρόντα κανονισμό. Μόνη εξαίρεση (παρ. 2 του ίδιου άρθρου) συνιστά η περίπτωση, κατά την οποία οι πάροχοι υπηρεσιών εμπιστοσύνης ενημερώνουν εκ των προτέρων και με τον αρμόζοντα τρόπο τους πελάτες τους σχετικά με τους αναφερόμενους περιορισμούς. Ειδικότερα, όσον αφορά στη χρήση των υπηρεσιών που παρέχουν και στις περιπτώσεις που οι περιορισμοί αυτοί είναι αναγνωρίσιμοι στους τρίτους, οι πάροχοι υπηρεσιών εμπιστοσύνης δεν ευθύνονται για ζημίες που προκαλούνται από χρήση των υπηρεσιών καθ' υπέρβαση των δηλωθέντων περιορισμών. Μάλιστα, στο ίδιο άρθρο προσδιορίζεται ακόμα και η αμέλεια που ενδέχεται να επιδείξουν, ενώ ρητώς αναφέρεται, ότι η ευθύνη των παρόχων κρίνεται σύμφωνα με το εθνικό δίκαιο του κάθε κράτους μέλους.

Ειδικότερα, λοιπόν, ευθύνη σε βάρος του παρόχου υπηρεσιών εμπιστοσύνης μπορεί να στοιχειοθετηθεί από οποιαδήποτε παραβίαση των υποχρεώσεων του, είτε αυτές τίθενται από συγκεκριμένες διατάξεις, είτε πρόκειται επί της ουσίας για ματαίωση της προσδοκίας του βασιζόμενου μέρους για καλόπιστη παροχή των υπηρεσιών.

Οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης ευθύνονται για τις περιπτώσεις μη τήρησης των απαιτήσεων ασφαλείας που θέτει το άρθρο 19. Πιο συγκεκριμένα, αυτοί οφείλουν να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα διαχείρισης των κινδύνων για την ασφάλεια των υπηρεσιών εμπιστοσύνης που παρέχουν. Λαμβανομένων υπόψη των τελευταίων τεχνολογικών εξελίξεων, τα εν λόγω μέτρα διασφαλίζουν ότι το επίπεδο ασφαλείας είναι ανάλογο προς τον βαθμό του κινδύνου. Συγκεκριμένα, λαμβάνονται μέτρα για την πρόληψη και την ελαχιστοποίηση του αντικτύπου των συμβάντων που άπτονται της ασφάλειας, καθώς και για την ενημέρωση των ενδιαφερομένων σχετικά με τις δυσμενείς επιπτώσεις τυχόν παρόμοιων συμβάντων. Ταυτόχρονα δε οι πάροχοι οφείλουν να ενημερώνουν το αργότερο εντός 24 ωρών αφότου έλαβαν γνώση, τους αρμόδιους φορείς, αλλά και το βασιζόμενο μέρος που απολαμβάνει τις παρεχόμενες υπηρεσίες, για οποιαδήποτε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας, που έχει σημαντικό αντίκτυπο στην παρεχόμενη υπηρεσία εμπιστοσύνης ή στα σχετικά δεδομένα προσωπικού χαρακτήρα.

Πέραν όμως αυτών των ανωτέρω υποχρεώσεων και ευθυνών, ειδικά οι εγκεκριμένοι πάροχοι οφείλουν, όπως συμμορφώνονται στις απαιτήσεις του Κανονισμού. Έτσι, στο άρθρο 24 περιγράφονται οι απαιτήσεις απέναντι στους παρόχους, ενώ τυχόν μη εκπλήρωσή τους, αυτομάτως συνιστά παραβίαση οποιασδήποτε διάταξης του στοιχειοθετεί αδικοπρακτική ευθύνη σε βάρος τους. Έτσι, κατά τις διατάξεις του προαναφερθέντος άρθρου ισχύουν τα κάτωθι:

«1. Κατά την έκδοση εγκεκριμένου πιστοποιητικού για υπηρεσία εμπιστοσύνης, ο εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης προβαίνει, με κατάλληλα μέσα και σύμφωνα με το εθνικό δίκαιο, σε εξακρίβωση της ταυτότητας και, κατά περίπτωση, τυχόν ειδικών χαρακτηριστικών του φυσικού ή νομικού προσώπου για το οποίο εκδίδεται εγκεκριμένο πιστοποιητικό.

Οι πληροφορίες που αναφέρονται στο πρώτο εδάφιο εξακριβώνονται από τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, είτε άμεσα είτε μέσω τρίτου σύμφωνα με το εθνικό δίκαιο:

α) με φυσική παρουσία του φυσικού προσώπου ή εξουσιοδοτημένου εκπροσώπου του νομικού προσώπου, ή

β) εξ αποστάσεως, με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης για τα οποία, πριν από την έκδοση του εγκεκριμένου πιστοποιητικού, έχει διασφαλιστεί η φυσική παρουσία του φυσικού προσώπου ή εξουσιοδοτημένου εκπροσώπου του νομικού

προσώπου και τα οποία πληρούν τις απαιτήσεις του άρθρου 8 όσον αφορά το «βασικό» ή το «υψηλό» επίπεδο διασφάλισης, ή

γ) μέσω πιστοποιητικού εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας που έχει εκδοθεί σύμφωνα με το στοιχείο α) ή β), ή

δ) με τη χρήση άλλων μεθόδων ταυτοποίησης αναγνωρισμένων σε εθνικό επίπεδο που παρέχουν διασφάλιση ισοδύναμη με τη φυσική παρουσία. Η ισοδύναμη διασφάλιση επιβεβαιώνεται από οργανισμό αξιολόγησης της συμμόρφωσης.

2. Οι εγκεκριμένοι πάροχοι υπηρεσιών που παρέχουν εγκεκριμένες υπηρεσίες εμπιστοσύνης:

α) ενημερώνουν τον εποπτικό φορέα για κάθε αλλαγή όσον αφορά στην παροχή των εγκεκριμένων υπηρεσιών εμπιστοσύνης του, περιλαμβανομένης της πρόθεσης παύσης των εν λόγω δραστηριοτήτων·

β) απασχολούν προσωπικό και, κατά περίπτωση, υπεργολάβους που διαθέτουν την απαραίτητη τεχνογνωσία, αξιοπιστία, πείρα και προσόντα και έχουν λάβει κατάλληλη εκπαίδευση, σχετικά με την ασφάλεια και τους κανόνες προστασίας των δεδομένων προσωπικού χαρακτήρα, εφαρμόζουν δε διοικητικές και διαχειριστικές διαδικασίες που ανταποκρίνονται σε ευρωπαϊκά ή διεθνή πρότυπα·

γ) όσον αφορά στην ευθύνη για τις ζημίες, σύμφωνα με το άρθρο 13, διατηρούν επαρκείς οικονομικούς πόρους και/ή αποκτούν κατάλληλη ασφαλιστική κάλυψη, σύμφωνα με το εθνικό δίκαιο·

δ) προτού συνάψουν συμβατική σχέση, ενημερώνουν, με σαφή και ολοκληρωμένο τρόπο, κάθε πρόσωπο που επιθυμεί να χρησιμοποιήσει εγκεκριμένη υπηρεσία εμπιστοσύνης, σχετικά με τους ακριβείς όρους και τις προϋποθέσεις για τη χρήση της εν λόγω υπηρεσίας, συμπεριλαμβανομένων τυχόν περιορισμών όσον αφορά στη χρήση της·

ε) χρησιμοποιούν αξιόπιστα συστήματα και προϊόντα τα οποία προστατεύονται από τροποποιήσεις και διασφαλίζουν την τεχνική ασφάλεια και αξιοπιστία των διεργασιών που υποστηρίζονται από αυτά·

στ) χρησιμοποιούν αξιόπιστα συστήματα για την αποθήκευση των δεδομένων που τους παρέχονται, σε επαληθεύσιμη μορφή, ούτως ώστε:

i) να είναι δημοσίως διαθέσιμα για άντληση μόνον εφόσον έχει ληφθεί η συγκατάθεση του προσώπου, στο οποίο αναφέρονται τα δεδομένα,

ii) μόνον εξουσιοδοτημένα πρόσωπα να μπορούν να πραγματοποιούν καταχωρίσεις και τροποποιήσεις στα αποθηκευμένα δεδομένα,

iii) να μπορεί να ελέγχεται η αυθεντικότητα των δεδομένων·

ζ) λαμβάνουν κατάλληλα μέτρα κατά της πλαστογραφίας και της κλοπής δεδομένων·

η) καταγράφουν και διατηρούν προσβάσιμο για κατάλληλη χρονική περίοδο, ακόμη και μετά την παύση των δραστηριοτήτων του εγκεκριμένου παρόχου υπηρεσιών εμπιστοσύνης, το σύνολο των συναφών πληροφοριών που αφορούν δεδομένα τα οποία έχουν εκδοθεί και ληφθεί από τον εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης, ιδίως για την παροχή αποδεικτικών στοιχείων σε νομικές διαδικασίες και για τη διασφάλιση της συνέχειας της υπηρεσίας· η καταγραφή αυτή δύναται να πραγματοποιείται με ηλεκτρονικά μέσα·

θ) διαθέτουν ενημερωμένο σχέδιο τερματισμού με σκοπό την εξασφάλιση της συνέχειας της υπηρεσίας, σύμφωνα με διατάξεις ελεγμένες από τον εποπτικό φορέα δυνάμει του άρθρου 17 παρ. 4 στοιχείο θ)·

ι) εξασφαλίζουν τη νόμιμη επεξεργασία των δεδομένων προσωπικού χαρακτήρα σύμφωνα με την Οδηγία 95/46/ΕΚ (νυν Κανονισμός (Ε.Ε.) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου)·

ια) σε περίπτωση εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης που εκδίδουν εγκεκριμένα πιστοποιητικά, συγκροτούν βάση δεδομένων για τα πιστοποιητικά, την οποία τηρούν ενημερωμένη.

3. Όταν εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης, που εκδίδουν εγκεκριμένα πιστοποιητικά, αποφασίζουν να ανακαλέσουν ένα πιστοποιητικό, καταχωρίζουν την εν λόγω

ανάκληση στη βάση δεδομένων για τα πιστοποιητικά και δημοσιοποιούν την ανάκληση του πιστοποιητικού εγκαίρως και σε κάθε περίπτωση εντός 24 ωρών από την παραλαβή της αίτησης. Η ανάκληση αυτή αρχίζει να ισχύει αμέσως μετά τη δημοσιοποίησή της.

4. Αναφορικά με την παράγραφο 3, οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης που εκδίδουν εγκεκριμένα πιστοποιητικά, παρέχουν σε κάθε βασιζόμενο μέρος πληροφορίες για την ισχύ ή την ανάκληση των εγκεκριμένων πιστοποιητικών που έχουν εκδοθεί από αυτούς. Οι εν λόγω πληροφορίες είναι διαθέσιμες, τουλάχιστον για κάθε χωριστό πιστοποιητικό, ανά πάσα στιγμή και πέραν της περιόδου ισχύος του πιστοποιητικού, κατά τρόπο αυτοματοποιημένο που είναι αξιόπιστος, δωρεάν και αποτελεσματικός.

5. (ημερομηνία επίσκεψης …]»

3.2.2.7. Ο ρόλος της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), η οποία ήδη από το 2000 λειτουργεί ως ανεξάρτητη Αρχή (ν. 2867/2000[98]) αποτελεί τον Εθνικό Ρυθμιστή που ελέγχει, ρυθμίζει και εποπτεύει: (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Επιπλέον, η ΕΕΤΤ ασκεί τις αρμοδιότητες Επιτροπής Ανταγωνισμού στις εν λόγω αγορές. Αποστολή της είναι να εξασφαλίσει την πρόσβαση όλων σε μεγάλο εύρος δικτύων και υπηρεσιών επικοινωνίας, να προασπίσει τα δικαιώματα των καταναλωτών τηλεπικοινωνιακών και ταχυδρομικών υπηρεσιών, να ενημερώνει διαρκώς τους καταναλωτές για τα δικαιώματα και τις υποχρεώσεις τους.[99] Ήδη κατά το προηγούμενο νομοθετικό καθεστώς (άρθρο 4 παρ. 2 και 8 του ΠΔ 150/2001[100]) η Επιτροπή ανέλαβε τον (κατασταλτικό) έλεγχο και την εποπτεία των Παρόχων Υπηρεσιών Πιστοποίησης για τη συμμόρφωση των ασφαλών διατάξεων δημιουργίας υπογραφής. Μάλιστα, στα πλαίσια αυτά η Επιτροπή προέβη με την υπ' αρ. 2478/71/2002 απόφασή της στην έκδοση του Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής[101], στον οποίο αναλυτικώς ρυθμίζονταν θέματα, τα οποία άπτονταν των υπηρεσιών πιστοποίησης των ηλεκτρονικών υπογραφών, των (κατά το προηγούμενο νομοθετικό πλαίσιο) «Αναγνωρισμένων» Πιστοποιητικών, καθώς και την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής.

[98] ΦΕΚ 273/Α/19-12-2000 για την οργάνωση και τη λειτουργία τηλεπικοινωνιών και άλλες διατάξεις
[99] https://www.eett.gr/opencms/opencms/EETT/EETT/AboutEETT/ (ημερομηνία επίσκεψης 20-05-2020)
[100] Σύμφωνα δε με το άρθρο 12, εδ. κ του Ν. 3431/2006 η Αρχή εποπτεύει και ελέγχει τη χρήση του φάσματος επιβάλλοντας και τις σχετικές κυρώσεις, όπως αυτές προβλέπονται στο Άρθρο 63 του ίδιου Νόμου.
[101] ΦΕΚ 603/Β'/16-5-2002

Ειδικότερα η ΕΕΤΤ επιφορτίστηκε τη διαπίστωση της δημόσιας ασφάλειας της διάταξης δημιουργίας υπογραφής, ενώ μπορούσε και να εξουσιοδοτεί και άλλους δημόσιους ή ιδιωτικούς φορείς για τον εν λόγω έλεγχο. Επίσης, η ΕΕΤΤ είναι αρμόδια να επιβάλλει πρόστιμα στους ΠΥΠ που ενεργούν ως διαπιστευμένοι, ενώ δεν είναι, καθώς και να ενημερώνει την Ευρωπαϊκή Επιτροπή για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων στην Ελλάδα ΠΥΠ, καθώς και το ταχύτερο δυνατό για τυχόν αλλαγές στις παραπάνω πληροφορίες[102]. Μάλιστα, βάσει αποφάσεων της ίδιας Επιτροπής διαμορφώθηκε ήδη πριν τη θέση σε ισχύ το νέου Κανονισμού, ένα θεσμικό πλαίσιο δυνάμει του οποίου η ανεξάρτητη αυτή αρχή ήταν υπεύθυνη για: α) για την διαπίστωση της συμμόρφωσης προς τις "ασφαλείς διατάξεις δημιουργίας υπογραφής"[103], β) *-τη ρύθμιση θεμάτων σχετικά με τα αναγνωρισμένα πιστοποιητικά, β) την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα ΠΥΠ ηλεκτρονικής υπογραφής, οι οποίοι εκδίδουν αναγνωρισμένα ή μη πιστοποιητικά ή παρέχουν άλλες σχετικές με την ηλεκτρονική υπογραφή υπηρεσίες πιστοποίησης[104], γ) τον ορισμό και τη λειτουργία των εντεταλμένων φορέων για την Εθελοντική Διαπίστευση (των ΠΥΠ) και τον έλεγχο των προϊόντων (ασφαλών διατάξεων δημιουργίας υπογραφής και ασφαλών κρυπτογραφικών μονάδων)[105] και δ) την Εθελοντική Διαπίστευση των ΠΥΠ, καθώς και η ακολουθούμενη τεχνολογία για την υλοποίησή της[106].

Με τη θέση σε ισχύ του νέου Κανονισμού, η Επιτροπή αποτελεί το φορέα εκείνο, ο οποίος είναι επιφορτισμένος με τις υποχρεώσεις εποπτείας των Παρόχων, όπως αυτές αναφέρονται στο δεύτερο τμήμα του Κανονισμού.[107] Ειδικότερα, η ΕΕΤΤ, οφείλει να συμβάλει στη δημιουργία ενός «ισότιμου πλαισίου ασφάλειας και υπευθυνότητας για πράξεις και υπηρεσίες», ώστε να διαφυλαχτούν αφενός μεν τα συμφέροντα των χρηστών, αφετέρου δε να επιτευχθεί η εύρυθμη λειτουργία της αγοράς.[108] συμβάλλοντας, κατ' αυτόν τον τρόπο στην προστασία των χρηστών και στη λειτουργία της εσωτερικής αγοράς. Ειδικότερα, η Επιτροπή, όχι μόνο είναι αρμόδια για την αδειοδότητση των εγκεκριμένων παρόχων υπηρεσιών εμπιστοσύνης (προληπτικός έλεγχος), και [109], προβαίνει σε έλεγχο ότι οι παρεχόμενες υπηρεσίες πληρούν τις απαιτήσεις του Κανονισμού, ενώ αναφορικά με τους μη εγκεκριμένους παρόχους εκείνη λειτουργεί κατασταλτικά στις περιπτώσεις που εικάζεται ότι οι τελευταίοι παραβιάζουν τις

[102] Άρθρο 8 παρ. 2 και 3 του π.δ. 150/2001
[103] Υπ. Αριθ. 295/64/2003 Απόφαση της ΕΕΤΤ (ΦΕΚ 1730/Β/24-11-03)
[104] Υπ. Αριθ. 248/71/2002 Απόφαση της ΕΕΤΤ (ΦΕΚ 603/Β/16-5-2002)
[105] Υπ. Αριθ. 295/63/10-10-2003 Απόφαση της ΕΕΤΤ (ΦΕΚ 1730/Β/24-11-03).
[106] Υπ. Αριθ. 295/65/2003 Απόφαση της ΕΕΤΤ (ΦΕΚ 1730/Β/24-11-03) & η υπ. Αριθ. 308/37/2004 Απόφαση της ΕΕΤΤ (ΦΕΚ 601Β`/Β/23-04-2004)
[107] Άρθρα 17-19 του Κανονισμού 910/2014.
[108] Σκέψη 36 του Προοιμίου του Κανονισμού 910/2014.
[109] Άρθρο 17 παρ. 4ζ

οριζόμενες στο Κανονισμό υποχρεώσεις τους.[110] Μάλιστα, η ΕΕΤΤ τηρεί μητρώο των Παρόχων υπηρεσιών εμπιστοσύνης και ενημερώνει ως εθνικός εποπτικός φορέας τον κατάλογο εμπιστοσύνης, στον οποίο συμπεριλαμβάνονται πληροφορίες σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης, καθώς και πληροφορίες σχετικά με τις εγκεκριμένες υπηρεσίες εμπιστοσύνης που παρέχουν (άρθρο 17 παρ. 4η και άρθρο 22 του Κανονισμού 910/2014). Επιπλέον, η συγκεκριμένη ανεξάρτητη αρχή οφείλει κάθε έτος να υποβάλει έκθεση πεπραγμένων στην Επιτροπή[111], ενώ παράλληλα «συνδράμει» τους εποπτικούς φορείς άλλων κρατών μελών[112], για την πλέον αποτελεσματική εποπτεία της παροχής υπηρεσιών εμπιστοσύνης στην κοινή αγορά (άρθρο 17 παρ. 4α του Κανονισμού).[113] Τέλος, θα πρέπει να σημειωθεί ότι η Επιτροπή δια της αποφάσεώς της 837/1Β εξέδωσε τον «Κανονισμός Παροχής Υπηρεσιών Εμπιστοσύνης»[114] , προκειμένου να ρύθμιση ειδικότερων ζητημάτων των υπηρεσιών εμπιστοσύνης για τη βέλτιστη εφαρμογή στην ελληνική έννομη τάξη του Κανονισμού (Ε.Ε.) αρ. 910/2014.

Ανακεφαλαιώνοντας όλα τα ανωτέρω για τις περιπτώσεις των εγκεκριμένων ηλεκτρονικών υπογραφών, καταλήγουμε στο συμπέρασμα, ότι πρόκειται για την πλέον αξιόπιστη μέθοδο διαδικασίας επιβεβαίωσης, όχι μόνο της ταυτότητας του αποστολέα, αλλά και της διατήρησης γνησιότητας του εγγράφου. Παρότι ο Κανονισμός (Ε.Ε.) 910/2014 παραμένει τεχνολογικά ουδέτερος, χωρίς να προσδιορίζει τα μέσα που χρησιμοποιούνται, θέτει μόνο τα ελάχιστα τεχνικά εχέγγυα παραγωγής ηλεκτρονικής υπογραφής, η οποία, όχι μόνο θα εκπληρώνει τους στόχους της προηγμένης ηλεκτρονικής υπογραφής, αλλά ταυτόχρονα δημιουργεί ένα πλέγμα διατάξεων και απαιτήσεων ασφαλείας για την παραγωγή της. Ταυτόχρονα δε, χορηγεί τα

[110] Άρθρο 17 παρ. 3 και σκέψη 36 του Κανονισμού 910/2014 . Η ανωτέρω διάκριση βέβαια εδράζεται στη βούληση του κοινοτικού νομοθέτη, ο οποίος στην ίδια σκέψη του Προοιμίου αναφέρει: «Οι μη εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης θα πρέπει να υπόκεινται σε ήπιες και αντενεργές εκ των υστέρων εποπτικές δραστηριότητες, δικαιολογούμενες από τη φύση των υπηρεσιών και των πράξεων. Ως εκ τούτου, ο εποπτικός φορέας δεν θα πρέπει να φέρει γενική ευθύνη εποπτείας μη εγκεκριμένων παρόχων υπηρεσιών. Ο εποπτικός φορέας θα πρέπει να αναλαμβάνει δράση μόνο όταν πληροφορείται (για παράδειγμα από τον ίδιο τον μη εγκεκριμένο παροχή υπηρεσίας εμπιστοσύνης, από άλλον εποπτικό φορέα, μέσω ειδοποίησης από χρήστη ή επιχειρηματικό εταίρο ή κατόπιν έρευνας του ίδιου του φορέα) ότι μη εγκεκριμένος παροχής υπηρεσίας εμπιστοσύνης δεν συμμορφώνεται προς τις απαιτήσεις του παρόντος κανονισμού.»

[111] Άρθρο 17 παρ. 4δ και 6 του Κανονισμού

[112] Ιδίως δε στις περιπτώσεις παροχής υπηρεσιών από Πάροχο εγκατεστημένο στην Ελλάδα, ο αποδέκτης των υπηρεσιών του οποίου είναι σε άλλο κράτος μέλος της Ένωσης (άρθρο 18 του Κανονισμού 910/2014).

[113] Άρθρο 17 παρ. 4. Βλ και σκέψη 40 του προοιμίου του Κανονισμού 910/2014: «Αυτό θα συνέβαλε στη διευκόλυνση της ανταλλαγής ορθών πρακτικών μεταξύ των εποπτικών φορέων και θα επιβεβαίωνε ότι οι βασικές απαιτήσεις εποπτείας εφαρμόζονται με συνέπεια και αποτελεσματικότητα σε όλα τα κράτη μέλη.»

[114] ΦΕΚ 4396/Β/14-12-2017

εχέγγυα μιας ελεγχόμενης διαδικασίας δημιουργίας της, μέσω της εποπτείας των «ανεξάρτητων τρίτων»- εγκεκριμένων Παρόχων υπηρεσιών εμπιστοσύνης, αλλά και των προϊόντων που αυτοί διαθέτουν στους τελικούς χρήστες-ηλεκτρονικά υπογράφοντες. Γι αυτούς τους λόγους η εγκεκριμένη ηλεκτρονική υπογραφή εξισώνεται εκ του νόμου με την ιδιόχειρη (άρθρο 25 του Κανονισμού).

3.2.3. Οι απλές ηλεκτρονικές υπογραφές

Η «απλές» ηλεκτρονικές υπογραφές εξετάζονται τελευταίες, καθώς αποτελούν ευρύτερη έννοια των ήδη αναλυθεισών περιπτώσεων, καθώς και γιατί όπως θα αναπτυχθεί ενδέχεται να μην έχουν όλες τις απαραίτητες ιδιότητες ασφάλειας που απαιτούνται από τις ηλεκτρονικές υπογραφές.

Ειδικότερα, αυτές προσδιορίζονται από το άρθρο 3 παράγραφο 12 του Κανονισμού και τους αποδίδεται ο βασικός ορισμός, όπως αυτός αναλύθηκε στο κεφάλαιο 3. Η δε αναγνώρισή τους ερείδεται στα οριζόμενα του άρθρο 25 παρ. 1 του Κανονισμού, όπως συνάγεται από το άρθρο 25 παρ. 1 του Κανονισμού 910/2014/Ε.Ε.: «Δεν απορρίπτεται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές υπογραφές.».

Το γεγονός ότι πρόκειται για συνειδητή επιλογή του ενωσιακού νομοθέτη, αποδεικνύεται και από το γεγονός ότι η υπό εξέταση κατηγορία, όπως ήδη αναφέρθηκε, εντοπίζεται και κατά την προϊσχύουσα Οδηγία 99/93/ΕΚ (άρθρο 5), όσο και στην «αινιγματική» διάταξη του άρθρου 3 παρ. 1 του πδ 150/2001.[115] Παρατηρείται λοιπόν, η σταθερή βούληση του νομοθέτη αναγνώρισης μίας τεχνολογικά ουδέτερης κατηγορίας υπογραφών, οι οποίες θα είναι σε θέση να παράγουν έννομα αποτελέσματα. Όπως επισημαίνεται και στον Κανονισμό, εναπόκειται στα δικαστήρια να κρίνουν κατά πόσο μπορεί να πληρείται έστω και ένα ελάχιστο επίπεδο ασφαλείας, ώστε πράγματι να μπορούν να εκπληρώνονται (έστω και ως ένα βαθμό) οι τέσσερις στόχοι της ηλεκτρονικής υπογραφής.

Έχει υποστηριχθεί δε ότι οποιαδήποτε δεδομένα συνημμένα σε άλλα, μπορούν να λειτουργήσουν ως ηλεκτρονικές υπογραφές, εφόσον μπορεί να διαπιστωθεί η βούληση του υπογράφοντος να δεσμευτεί από το περιεχόμενο του ηλεκτρονικού εγγράφου, αναλαμβάνοντας όμως σε κάθε περίπτωση και την έκθεσή του στους κινδύνους του ψηφιακού περιβάλλοντος,

[115] Κ. Δελούκα – Ιγγλέση, ό.π., σ. 211-212.

ως ήδη αναφέρθηκαν[116] Ενδεικτικά ορισμένες περιπτώσεις[117] εξομοιωμένες με τις ηλεκτρονικές υπογραφές μπορούν να θεωρηθούν οι κάτωθι:

1. η απλή ηλεκτρονική αναφορά του ονόματος του συγγραφέα στο τέλος ενός ηλεκτρονικού εγγράφου,

2. η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση που έχει οριστεί και χρησιμοποιηθεί από τον ίδιο τον αποστολέα ενός e-mail,[118]

3. μία ψηφιακή εικόνα χειρόγραφης υπογραφής που προσαρτάται στο τέλος ενός ηλεκτρονικού αρχείου,

4. η επιλογή με το «ποντίκι» του Η/Υ του εικονιδίου «ναι» (ως πράξη αποδοχής) σε μια ιστοσελίδα κατά την κατάρτιση ηλεκτρονικής σύβασης μεταξύ καταναλωτή – προμηθευτή

5. ένα «σήμα» που ο αποστολέας το χρησιμοποιεί για να αυτοσυστήνεται, όπως ένας ήχος ή μία εικόνα.

Μόνο από την αναφορά ορισμένων εξ αυτών καθίσταται πασίδηλο, βάσει των διδαγμάτων της κοινής πείρας, ότι εάν όχι κανένας, τότε ελάχιστοι από τους επιθυμητούς σκοπούς της ηλεκτρονικής υπογραφής εξυπηρετούνται. Επιπλέον, στις περιπτώσεις αυτές η ηλεκτρονική υπογραφή παύει να είναι μία σύναψη απόρρητων δεδομένων του υπογράφοντος με τα δεδομένα – ηλεκτρονικό έγγραφο προς υπογραφή.

Εν τούτοις, όπως θα αναλυθεί και στο επόμενο κεφάλαιο, παρά τις ελάχιστες εγγυήσεις οι «απλές ηλεκτρονικές υπογραφές» φαίνεται υπό περιστάσεις, παρά την έλλειψη ασφαλείας, ότι αναγνωρίζονται από την ελληνική έννομη τάξη. Ειδικότερα, όπως έχει αναφερθεί ήδη, το περιεχόμενο των ηλεκτρονικών εγγράφων επί της ουσίας περιέχει την εκπεφρασμένη βούληση του χρήστη στο ψηφιακό περιβάλλον. Μάλιστα, επισημάνθηκε ότι δεν είναι αναγκαίο η βούληση αυτή να είναι απευθυνθεί σε συγκεκριμένο πρόσωπο ή να αναμένεται ορισμένη απάντηση σε αυτή. Επιπλέον, βασική αρχή του ουσιαστικού αστικού δικαίου αναφορικά με τις συμβάσεις είναι το άτυπο αυτών (άρθρο 158 ΑΚ). Για αυτές τις περιπτώσεις λοιπόν, δικαιολογημένα υποστήριξε η

[116] Μητρακάς Α., ό.π., σ. 112-113, αλλά και Ι. Ιγγλεζάκης, ό.π., σ. 224επ., όπου σημειώνεται: «(…) η «απλή» ηλεκτρονική υπογραφή μπορεί να παρέχει τα εχέγγυα για την εγκυρότητα των συμβάσεων για τις οποίες δεν προβλέπεται έγκυρος τύπος, αφού ο κανόνας είναι το άτυπο των δικαιοπραξιών, σύμφωνα με 158ΑΚ. (…)»

[117] Κοσμάς Α. Καραδημητρίου, υπ., σ. 51-53

[118] Βλ. σχετικά Γ. Ζέκο, υπ., σ. 73επ., ο οποίος αναφέρει ότι «η τεχνική αποστολής του ηλεκτρονικού ταχυδρομείου οδηγεί υποχρεωτικά στην ταύτιση μηνύματος και αποστολέα, με συνέπεια, κατά την αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου, η δήλωση βούλησης του αποστολέα να ταυτίζεται με την ηλεκτρονική του διεύθυνση και να καθίσταται ένα ενιαίο σύνολο.»

θεωρία[119] τη χρήση υπογραφών πέραν των αναλυθεισών ηλεκτρονικών συνάψεων ότι αυτές μπορούν να υποκαταστήσουν το ρόλο της υπογραφής για το κύρος των ηλεκτρονικών εγγράφων. Σε επίπεδο δε δικονομικού δικαίου, ήδη αναπτύχθηκε ότι το δικαστήριο δεν δεσμεύεται στην κρίση του από περιεχόμενο που αναφέρεται στο ηλεκτρονικό έγγραφο, ανεξαρτήτως της ύπαρξης ή μη υπογραφής. Ωστόσο, στην περίπτωση που η τελευταία υπάρχει, τότε το αποδεικτικό μέσο αξιολογείται διαφορετικά, αφού στην περίπτωση ιδιόχειρης υπογραφής ή εξομοιωμένης με την τελευταία ηλεκτρονικής, τότε το έγγραφο αξιολογείται δυνάμει του άρθρου 445 ΚΠολΔ. Αντίθετα, στις περιπτώσεις των απλών ηλεκτρονικών υπογραφών το δικαστήριο θα πρέπει να κρίνει το αποδεικτικό μέσο δυνάμει του άρθρου 448 παρ. 3 του ΚΠολΔ, «εφόσον αποδεικνύεται ύπαρξη τελολογικού υποκατάστατου της ιδιόχειρης υπογραφής».[120]

[119] Ε. Φιλιποπούλου ό.π.1091-1092, Ομοίως Κ. Δελούκα-Ιγγλέση, ό.π., σ. 206 επ. και Ι. Ιγγλεζάκης, ό.π., σ. 224 επ. (βλ. και υποσημείωση παρούσας 115).

[120] Κ. Δελούκα–Ιγλλέση, ό.π., σ. 212-213. Βλ. και Ι. Ιγγλεζάκη, ό.π. σ. 224 επ., όπου υποστηρίζεται ότι μετά τις τροποποιήσεις που επέφερε ο ν. 3994/2011 (άρθρο 40 παρ. 2), το έγγραφο, το οποίο φέρει απλή ηλεκτρονική υπογραφή μπορεί να χρησιμοποιηθεί ως αποδεικτικό έγγραφο κατ' άρθρον 444 αρ. 2 ΚΠολΔ,, εφόσον πλέον εμπίπτει στην έννοια των μηχανικών απεικονίσεων.

Κεφάλαιο 4ο: Επισκόπηση νομοθεσίας και νομολογίας για τις ηλεκτρονικές υπογραφές.

Στο παρόν κεφάλαιο εξετάζεται με τρόπο συνοπτικό, τόσο το προϊσχύον δίκαιο, όσο και το υφιστάμενο, προκειμένου να μπορέσουν να εξαχθούν συμπεράσματα σχετικά με τη λειτουργία των ηλεκτρονικών υπογραφών. Η ανάλυση που ακολουθεί, δεν αποσκοπεί στην αναλυτική περιγραφή του εκάστοτε νομοθετικού πλαισίου. Αντιθέτως, επισημαίνονται τα καίρια σημεία του κάθε νομοθετήματος (θετικά και αρνητικά) προκειμένου να καταστεί αντιληπτή η συνεισφορά του Κανονισμού (Ε.Ε.) 910/2014 στο υπό εξέταση θέμα, καθώς και να αναδειχθούν τυχόν αρνητικές πτυχές του. Τέλος, στην υποενότητα 5.3. πρόκειται να παρουσιαστεί μία επισκόπηση της νομολογίας των ελληνικών πολιτικών δικαστηρίων, προκειμένου να εξαχθούν συμπεράσματα για την αντιμετώπιση του νομικού ζητήματος των ηλεκτρονικών υπογραφών από τα ελληνικά δικαστήρια.

4.1. Κριτική επισκόπηση του προϊσχύοντος δικαίου

Στην ενότητα αυτή επιχειρείται μία κριτική επισκόπηση της Οδηγίας 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθώς και του π.δ. 150/2001 με το οποίο ενσωματώθηκε η ανωτέρω Οδηγία στο εθνικό δίκαιο.

4.1.1. Κριτική επισκόπηση της Οδηγίας 99/93/ΕΚ

Με τη θέση σε ισχύ της Οδηγία 99/93/Ε.Κ. επιχειρήθηκε, όπως υπάρξει η προσέγγιση μίας κοινής – σε ευρωπαϊκό επίπεδο – λύσης για τα προβλήματα που αντιμετώπιζε (και) η ευρωπαϊκή έννομη τάξη κατά τις ηλεκτρονικές συνδιαλλαγές, αλλά και συναλλαγές. Συνεπώς, η θέσπιση ενός σύγχρονου και ομοιόμορφου πλαισίου σχετικά με τις ηλεκτρονικές υπογραφές, θα παρείχε στο συναλλασσόμενο τη δυνατότητα να συναλλάσσεται χωρίς όρια, αλλά και με ασφάλεια στην παγκόσμια ηλεκτρονική αγορά.

Αυτό πραγματοποιήθηκε αρχικά με την Οδηγία 99/93/Ε.Κ. του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου η οποία ψηφίστηκε το Δεκέμβριο του 1999. Η Οδηγία είχε ως στόχο να δημιουργήσει ένα σαφές, κοινοτικό πεδίο ρύθμισης των ηλεκτρονικών υπογραφών και των υπηρεσιών πιστοποίησης, για να ενισχυθεί η εμπιστοσύνη στις νέες τεχνολογίες.[121] Δηλώνεται δε εκ Προοιμίου[122], ότι η Οδηγία 99/93/Ε.Κ. δεν αφορά τον τύπο των ενοχικών συμβάσεων, ούτε αποσκοπεί στην ρύθμισή τους. Έτσι, συμπεραίνεται ότι οι ρύθμιση των ηλεκτρονικών υπογραφών αφορούσε τις περιπτώσεις, κατά τις οποίες η έννομη τάξη του κάθε κράτους

[121] Αιτιολογική σκέψη 4 του Προοιμίου της Οδηγίας 99/93/Ε.Κ.
[122] Αιτιολογική σκέψη 1 του Προοιμίου της Οδηγίας 99/93/Ε.Κ.

μέλους, απαιτούσε ένα νομικό ισοδύναμο, το οποίο θα κάλυπτε τις λειτουργίες των ιδιόχειρων υπογραφών.

Μάλιστα, ήδη από το Προοίμιο της Οδηγία 99/93/Ε.Κ. ο κοινοτικός νομοθέτης ξεκάθαρα λαμβάνει θέση υπέρ μίας ανοιχτής στις νέες τεχνολογίες προσέγγιση των ηλεκτρονικών υπογραφών.[123] Ταυτόχρονα, όμως όπως αναφέρθηκε ήδη απαιτείτο η μέγιστη δυνατή ασφάλεια για τις περιπτώσεις εκείνες που η ηλεκτρονική υπογραφή θα εξισωνόταν με τις ιδιόχειρες υπογραφές. Αυτό οδήγησε δε στην υβριδική προσέγγιση των ηλεκτρονικών υπογραφών. Από τη μία δηλαδή υιοθετήθηκε μία μινιμαλιστική προσέγγιση των ηλεκτρονικών υπογραφών, αναγνωρίζοντας νομική αναγνώριση σε όλες τις μορφές των ηλεκτρονικών υπογραφών, ανεξαρτήτως των προδιαγραφών τους.[124] Ταυτόχρονα όμως, προκειμένου να επιτευχθεί το μέγιστο επίπεδο ασφάλειας, παρατηρείται στην περίπτωση των αναγνωρισμένων προηγμένων ηλεκτρονικών υπογραφών (νυν εγκεκριμένων) η απαίτηση αυτές να πληρούν μία σειρά νομικών όρων.[125] Αυτή η προσέγγιση λοιπόν, ήδη υπό το προισχύσαν θεσμικό πλαίσιο οδήγησε στην νομική αναγνώριση τόσο των απλών ηλεκτρονικών υπογραφών, όσο και των αναγνωρισμένων, ικανών να παράγουν έννομα αποτελέσματα, αφήνοντας δε στη διακριτική ευκαιρία των εθνικών δικαστηρίων να κρίνουν κατά πόσο η μία ή άλλη κατηγορία υπογραφών μπορούσε να πληροί τις προϋποθέσεις για την έγκυρη σύναψη των συμβάσεων.[126]

Επίσης, δεδομένων των ρυθμίσεων και των προϋποθέσεων που τάχθηκαν για τις αναγνωρισμένες (προηγμένες) ηλεκτρονικές υπογραφές, καθοριστικής σημασίας υπήρξαν οι ρυθμίσεις που προβλέφθηκαν για τους έμπιστους τρίτους φορείς, ήτοι των Παρόχων Υπηρεσιών Πιστοποίησης (νυν εγκεκριμένοι φορείς παροχής υπηρεσιών εμπιστοσύνης). Ειδικότερα, ο κοινοτικός νομοθέτης αναγνωρίζοντας το ρόλο τους για την εμπέδωση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές, δημιούργησε ένα ελάχιστο πλέγμα υποχρεώσεων των Παρόχων. Με την εισαγωγή μάλιστα νόθου αντικειμενικής ευθύνης (άρθρο 6 της Οδηγία 99/93/Ε.Κ.) συνέβαλε στην ενίσχυση της εμπιστοσύνη των καταναλωτών απέναντι στους τελευταίους.[127]

Αναφορικά με τις Παρόδους Υπηρεσιών Πιστοποίησης τομή αποτέλεσαν οι τέσσερις αρχές που υιοθετηθήκαν[128]. Ειδικότερα, οι αρχές αυτές είναι:

[123] Βλ. αιτιολογική σκέψη 8 του Προοιμίου της Οδηγίας 99/93/Ε.Κ.
[124] Κοσμάς Α. Καραδημητρίου,ό.π., σ. 124
[125] Σιούλης Χ., ό.π.2-3
[126] Κ. Δελούκα–Ιγγλέση, ό.π. , σ. 210-2013
[127] Κοσμάς Α. Καραδημητρίου, ό.π., 202-204
[128] Κ. Δελούκα–Ιγγλέση, ό.π. , σ. 199-201

α) Η αρχή της μη προηγούμενης εγκρίσεως (άρθρο 3 παρ. 1): Σύμφωνα με αυτή «τα κράτη μέλη δεν εξαρτούν την παροχή υπηρεσιών πιστοποίησης από εκ των προτέρων έγκριση».[129] Θεωρήθηκε δηλαδή ότι έτσι θα δημιουργηθεί ανταγωνισμός μεταξύ των ΠΥΠ, ο οποίος θα λειτουργούσε προς όφελος των καταναλωτών και των επιχειρήσεων, αφού θα η απουσία των πολυδάπανων και χρονοβόρων αδειοδοτήσεων των ΠΥΠ θα εξασφάλιζε την ανάπτυξη της επιχειρηματικής δραστηριότητας των Παρόχων στο εσωτερικό κάθε χώρας.[130]

β) Η αρχή της εθελοντικής διαπίστευσης (άρθρο 3 παρ. 2): Μέγιστο θέμα για την ποιότητα των παρεχόμενων υπηρεσιών πιστοποίησης συνιστά ο έλεγχος από αρμόδια όργανα. Κατ' επιλογήτου Κοινοτικού νομοθέτη η επίτευξη ενός βελτιωμένου επιπέδου παροχής υπηρεσιών επιτυγχανόταν μέσω του ελέγχου των υπηρεσιών των Παρόχων από το αρμόδιο κρατικό φορέα[131]

γ) Η αρχή επιτήρησης για τα αναγνωρισμένα πιστοποιητικά (άρθρο 3 παρ. 3): Η εν λόγω αρχή αφορά την υποχρέωση των κρατών μελών, όπως υιοθετήσουν ένα σύστημα επιτήρησης των παρόχων υπηρεσιών πιστοποίησης, οι οποίοι εκδίδουν τα κοινά αναγνωρισμένα πιστοποιητικά.[132]

δ) Η αρχή της χώρας προέλευσης (άρθρο 4 παρ. 1): Εφόσον οι Πάροχοι ενός κράτους-μέλους μπορούσαν να παρέχουν τις υπηρεσίες τους σε καταναλωτές έτερων κρατών μελών, υιοθετήθηκε η συγκεκριμένη αρχή, με αποτέλεσμα το δίκαιο παροχής των υπηρεσιών να διέπεται από το δίκαιο του κράτους μέλους προέλευσης των παρεχόμενων υπηρεσιών.

Παρά το γεγονός ότι η συνεισφορά της Οδηγία 99/93/Ε.Κ. αποτιμάται θετικά, παρατηρήθηκε ότι με τη θέσπιση της Οδηγία 99/93/Ε.Κ. υπήρξαν ορισμένες προσδοκίες ότι το νομοθετικό

---

[129] Στην Ελλάδα, βάσει της υπ. αριθ. 248/71/2002 Απόφασης της ΕΕΤΤ (ΦΕΚ 603/Β/16-5-2002) μόνη υποχρέωση των ΠΥΠ που εξέδιδαν πιστοποιητικά ηλεκτρονικών υπογραφών (ακόμη και μη «αναγνωρισμένα») υποχρεούντο σε 'ανακοίνωση της έναρξης παροχής των υπηρεσιών' τους και στην εγγραφή τους σε σχετικό 'μητρώο' που δημοσιεύει η ΕΕΤΤ.

[130] Αιτιολογική σκέψη 10 της Οδηγίας.

[131] Η θέση αυτή του νομοθέτη έχει ιδιαιτέρως επικριθεί από τη θεωρία, καθώς θεωρήθηκε ότι, η απουσία συγκεκριμένου πλαισίου για μία ενιαία αντιμετώπιση, θα ήταν επικίνδυνη, λόγω των ανισοτήτων που θα δημιουργούνταν από τον καθορισμό διαφορετικών προϋποθέσεων από το κάθε κράτος - μέλος. Βλ. σχετικά Β. Καραγιάννη, Το κοινοτικό νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές - Η Οδηγία 1999/93/Ε.Κ., ΔΕΕ 6/2000, σ. 587, αλλά και Κ. Καραδημητρίου ό.π. σ. 148, όπου επισημαίνεται ο κίνδυνος ενός de facto περιορισμού της εθελοντικής διαπίστευσης, εφόσον μόνο οι εθελοντικώς διαπιστευμένοι φορείς πληρούσαν τα κριτήρια για τη δημιουργία της εγκεκριμένης ηλεκτρονικής υπογραφής. Ειδικότερα, όπως αναφέρει: «Στην καθημερινή πρακτική, δηλαδή, ο ΠΥΠ που επιθυμεί να Εκμεταλλευθεί εμπορικά τα ειδικά νομικά οφέλη της προηγμένης ηλεκτρονικής υπογραφής που εξισώνεται μ ε την ιδιόχειρη, πιθανότατα θα υποχρεωθεί εκ των πραγμάτων να ενταχθεί στο σύστημα της εθελοντικής διαπίστευσης, γεγονός που ίσως να δημιουργήσει έναν άτυπο «εμπορικό μονόδρομο» για τους ΠΥΠ, κάτι που, τελικά, δεν απέχει πολύ από ένα καθεστώς κρατικής αδειοδότησης των ΠΥΠ»

[132] Ως ήδη αναφέρθηκε στην ενότητα 4.2.2.6. ενόψει των διατάξεων των παραγράφων 2 και 8 του άρθρου 4 του πδ 150/2001

αυτό μέτρο θα συνέβαλε στην απογείωση της αγοράς ηλεκτρονικής υπογραφής, πράγμα το οποίο δεν συνέβη.[133] Ειδικότερα, παρατηρήθηκαν αστοχίες, όσον αφορά τόσο τις νομικές ρυθμίσεις, όσο όμως και τεχνικά ζητήματα, τα οποία όμως εδώ παραλείπονται ως μη σχετιζόμενα με το ερευνόμενο αντικείμενο. Οι πλέον βασικές των κατηγοριών που δέχτηκε η Οδηγία 99/93/Ε.Κ. αναφέρονται συνοπτικά ακολούθως.

Α) Από τις διατάξεις της Οδηγία 99/93/Ε.Κ. προκύπτει μία εκτενής κατηγοριοποίηση των ηλεκτρονικών υπογραφών. Ειδικότερα, με το προϊσχύον δίκαιο αναγνωρίζονταν:
α) οι απλές ηλεκτρονικές υπογραφές (άρθρο 2 παρ. 1)
β) οι προηγμένες ηλεκτρονικές υπογραφές (άρθρο 2 παρ. 2)
γ) οι προηγμένες ηλεκτρονικές υπογραφές, οι οποίες αναγνωρίζονταν ως ισότιμες των ιδιόχειρων. Στην περίπτωση αυτή οι προηγμένες υπογραφές έπρεπε να υποστηρίζονται από αναγνωρισμένο πιστοποιητικό και να γίνεται χρήση ασφαλούς διάταξης δημιουργίας υπογραφής.
δ) μία ενδιάμεση κατηγορία των υπό β) και γ) περιπτώσεων, ήτοι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται μεν σε αναγνωρισμένο πιστοποιητικό, αλλά δεν παράγονται με «ασφαλή διάταξη δημιουργίας υπογραφής».[134]

Η εκτενής κατηγοριοποίηση αυτή, παρότι έχει χαιρετηθεί από μέρος της θεωρίας ως συμβάλλουσα στην ενίσχυση της αξιοπιστίας των ηλεκτρονικών υπογραφών, καθώς και της προστασίας του χρήστη-υπογράφοντος[135], από την άλλη μεριά δέχτηκε και δριμεία κριτική. Αρχικά, επρόκειτο για ένα αρκετά περίπλοκο σύστημα, το οποίο καθιστούσε εξαιρετικά δυσχερές ακόμα και για τους Παρόδους Υπηρεσιών Πιστοποίησης να μπορέσουν να ανταποκριθούν στο σύνολο των απαιτήσεων που έθετε η οδηγία. Ταυτόχρονα δε, παρατηρήθηκε[136] ότι έτσι δημιουργήθηκε ένα πολυδαίδαλο σύστημα, το οποίο προκαλούσε ιδιαίτερη δυσκολία στην παροχή υπηρεσιών που να ικανοποιούν όλες τις τεχνικές απαιτήσεις, ωθώντας του χρήστες σε άλλες μορφές ηλεκτρονικών υπογραφών (απλές).

---

[133] Επιτροπή των Ευρωπαϊκών Κοινοτήτων, 2006
[134] Βλ. αιτιολογική σκέψη 20 του Προοιμίου της Οδηγίας 99/93/Ε.Κ. «(…) οι προηγούμενες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό στοχεύουν (…)»
υψηλότερο επίπεδο ασφάλειας·
[135] Σιούλης Χ, ό.π., σ. 15
[136] Επιτροπή των Ευρωπαϊκών Κοινοτήτων (2006).COM(2006). Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Έκθεση αναφορικά με τη λειτουργία της οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. διαθέσιμο στην ηλεκτρονική διεύθυνση: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120: FIN:EL:PDF (ημερομηνία επίσκεψης 02-05-2020)

Β) Η Οδηγία 99/93/ΕΚ θέσπιζε, όπως αναφέρθηκε ανωτέρω, ήπιες μορφές ελέγχου των έμπιστων τρίτων παρόχων (Παρόχων Υπηρεσιών Πιστοποίησης). Με την πρόβλεψη για εθελοντική διαπίστευση, ο τυχόν προληπτικός έλεγχος καθίστατο προαιρετικός, όπερ και είχε προκαλέσει την κριτική της θεωρίας αναφορικά με την μη συμμόρφωσή τους με «κάποιους ελάχιστους κανόνες γενικού ενδιαφέροντος σε θέματα αξιοπιστίας και ασφάλειας των ηλεκτρονικών συναλλαγών)».[137] Συνεπώς, όσο και εάν αυτό ενίσχυε τον ανταγωνισμό της οικονομίας της αγοράς καθιστούσε τους καταναλωτές ευάλωτους στις περιπτώσεις που ο Παροχής στον οποίο απευθύνονταν δεν ανταποκρινόταν στις τεχνικές απαιτήσεις που έθετε ο νόμος για τις παρεχόμενες υπηρεσίες αναφορικά με τις ηλεκτρονικές υπογραφές. Ταυτόχρονα, διαπιστώθηκε ότι ο εποπτικός έλεγχος των Παρόχων από τους αρμόδιους κρατικούς φορείς υπήρξε αναποτελεσματικός (Επιτροπή των Ευρωπαϊκών Κοινοτήτων, 2006) με αποτέλεσμα να μην μπορεί να επιτευχθεί η διαλειτουργικότητα. Τέλος, στο ίδιο πλαίσιο πρόκλησης αβεβαιότητας εντάσσεται και η επιλογή του κοινοτικού νομοθέτη να απαλλάξει του Παρόχους Υπηρεσιών Πιστοποίησης από επιγενόμενο κίνδυνο για τις περιπτώσεις ακρίβειας και πληρότητας του χορηγούμενου πιστοποιητικού, αλλά και σε ό,τι αφορά την ταυτότητα του υπογράφοντος.[138] Εν προκειμένω, έχει υποστηριχτεί[139] ότι με αυτό τον τρόπο ο καταναλωτής – κάτοχο του πιστοποιητικού γνησιότητας ηλεκτρονικής υπογραφής ή ο καλόπιστος τρίτος αναλάμβαναν άκοντες τον επιγενόμενο κίνδυνο που προκαλούν οι συνεχείς τεχνολογικές εξελίξεις, ενώ μετακυλύετε σε αυτούς αποκλειστικά το οικονομικό βάρος ανόρθωσης τυχόν μελλοντικής τους ζημίας.

Συμπερασματικά, παρά την κριτική που ασκήθηκε στην εν λόγω Οδηγία 99/93/Ε.Κ. και τις τυχόν αστοχίες ως προς τον αντίκτυπό της στην «αγορά», θα πρέπει να σημειωθεί ότι χάρη στη συμβολή της εξασφαλίστηκε ασφάλεια δικαίου όσον αφορά τη γενική αποδοχή των ηλεκτρονικών υπογραφών και επιτεύχθηκε η νομική αναγνώρισή τους.[140]

4.1.2. Κριτική επισκόπηση του π.δ. 150/2001

Το π.δ. 150/2001 μετέφερε την Οδηγία 99/93/ΕΚ στην ελληνική έννομη τάξη. Όπως και σε αρκετές άλλες περιπτώσεις ευρωπαϊκών Οδηγιών, παρατηρήθηκε η σχεδόν τυφλή αναπαραγωγή του κοινοτικού κειμένου, διαψεύδοντας μέρος της θεωρίας, το οποίο ανέμενε μία προσαρμογή στα δεδομένα του ελληνικού (ουσιαστικού κυρίως) αστικού δικαίου.[141] Αυτό έχει ως συνέπεια βέβαια σε μεγάλο βαθμό να φέρει και το εν λόγω διάταγμα, όχι μόνο τα θετικά

[137] Καραγιάννης Β. (2000), Το κοινοτικό νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές - Η Οδηγία 1999/93/Ε.Κ.. ΔΕΕ 6/2000, σ. 580 επ.
[138] άρθρο 6 παρ. 1 της Οδηγίας 99/93/Ε.Κ.
[139] Κοσμάς Α. Καραδημητρίου, ό.π., σ. 200-201
140 Επιτροπή Ευρωπαϊκών Κοινοτήτων, ό.π.

[141] Χ. Μιχαηλίδου Χ., ό.π., σ. 6 επ.

στοιχεία της Οδηγία 99/93/Ε.Κ., αλλά κα όλες εκείνες τις διατάξεις που αποτέλεσαν στόχο κριτικής.

Ως προς τους ορισμούς που υιοθετεί σε σχέση με τις ηλεκτρονικές υπογραφές είναι αυτοί που ήδη αναλύθηκαν για τις κατηγορίες των ηλεκτρονικών υπογραφών που αναγνωρίζονται και με τον ισχύοντα Κανονισμό (Ε.Ε.) 910/2014. Η διαφορά έγκειται στις αναγνωρισμένες – προηγμένες ηλεκτρονικές υπογραφές, όπως αυτές πλέον ορίζονται ως «εγκεκριμένες ηλεκτρονικές υπογραφές». Ειδικότερα, όπως ήδη αναφέρθηκε, κατά το π.δ. 150/2001 (κατά πιστή μεταφορά της Οδηγία 99/93/Ε.Κ.) για να έχει η ηλεκτρονική υπογραφή ισχύ ισοδύναμη της ιδιόχειρης θα έπρεπε να βασίζεται σε αναγνωρισμένο πιστοποιητικό, ήτοι εκείνο που ανταποκρινόταν στις απαιτήσεις του Παραρτήματος Ι του διατάγματος, αλλά και να δημιουργείται από ασφαλή διάταξη υπογραφής, ήτοι να αξιοποιείται για τη δημιουργία διατεταγμένο υλικό ή λογισμικό, όπως η σημασία του έχει ήδη αναλυθεί ανωτέρω για την εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικών υπογραφών.

Ιδιαίτερη διαφοροποίηση, για την οποία επικρίθηκε εντόνως ο Έλληνας νομοθέτης [142], ήταν η επιλογή του να χαρακτηρίσει διαζευκτικώς τις προηγμένες ηλεκτρονικές υπογραφές ως ψηφιακές. Προέβη δηλαδή σε μία λανθασμένη ταύτιση της έννοιας της ψηφιακής υπογραφής (δηλαδή ηλεκτρονική υπογραφή παραγόμενη με τη μέθοδο της ασύμμετρης κρυπτογραφίας) με την προηγμένη ηλεκτρονική υπογραφή. Ωστόσο, η Οδηγία 99/93/Ε.Κ., υιοθετώντας τεχνολογικά ουδέτερη θέση, θέλησε να καλύψει κάθε ηλεκτρονική υπογραφή που μπορούσε να ικανοποιήσει τα κριτήρια της προηγμένης ηλεκτρονικής υπογραφής. Επρόκειτο λοιπόν για έναν αδικαιολόγητο περιορισμό.

Τέλος, ο Έλληνας νομοθέτης μετέφερε σχεδόν αυτούσιες τις διατάξεις της Οδηγία 99/93/Ε.Κ. στην ελληνική έννομη τάξη, με αποτέλεσμα να δεχτεί κριτική ότι δεν μερίμνησε να επιδείξει την ελάχιστη οφειλόμενη σαφήνεια. Ειδικότερα, όπως έχει επισημανθεί[143] η αναφορά του διατάγματος στο άρθρο 2 παρ. 1 για το ποιες κατηγορίες διατάξεων του εθνικού δικαίου δεν θίγονται από το π.δ. 150/2001 γίνεται με τρόπο τόσο γενικόλογο, ώστε να προτείνεται μία συμπληρωματική και διευκρινιστική διαφοροποίηση στο κείμενο.

4.2. Κριτική επισκόπηση του Κανονισμού (Ε.Ε.) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

Με τη θέση σε ισχύ της Οδηγίας 99/93/Ε.Κ., παρά το κεκτημένο που δημιούργησε ως προς τη χρήση των ηλεκτρονικών υπογραφών, διαπιστώθηκε ανομοιομορφία αναφορικά με την εφαρμογή των κοινοτικών διατάξεων. Επιπλέον, η υπερδεκαετής εφαρμογή του Κανονιστικού

[142] Κοσμάς Α. Καραδημητρίου , ό.π., σ. 121-123
[143] Κοσμάς Α. Καραδημητρίου , ό.π., σ.184 επ.

πλαισίου οδήγησε την Επιτροπή και το Ευρωπαϊκό Κοινοβούλιο σε συμπεράσματα σχετικά με τις τυχόν αδυναμίες του ισχύοντος ρυθμιστικού πλαισίου. Άλλωστε, όπως ήδη ανωτέρω επισημάνθηκε, το γεγονός ότι δεν είχαν υιοθετηθεί από όλα τα κράτη μέλη τα ίδια τεχνικά πρότυπα, αποτελούσε τροχοπέδη στην ανάπτυξη της διαλειτουργικότητας.

Τούτων δεδομένων, με τη θέσπιση του Κανονισμού (Ε.Ε.) 910/2014 με ημερομηνία εφαρμογής του από τα κράτη μέλη τον Ιούλιο του 2016 ο Κανονισμός (Ε.Ε.) 910/2014 κατήργησε την προϋφιστάμενη Οδηγία 99/93/Ε.Κ. αντικαθιστώντας τις διατάξεις του εθνικού δικαίου των κρατών μελών σε ό,τι αφορά τις ηλεκτρονικές υπογραφές. Στόχος .. δε του Κανονισμού[144] υπήρξε η ενίσχυση της εμπιστοσύνης στις ηλεκτρονικές συναλλαγές εντός της εσωτερικής αγοράς και η ενίσχυση του κεκτημένου των ηλεκτρονικών υπογραφών. Η (αναγκαστικά) μάλιστα ομοιόμορφη εφαρμογή ενός κοινού νομοθετικού πλαισίου οδήγησε συνέβαλε στην επίτευξη ενός ενιαίου ολοκληρωμένου διασυνοριακού πλαισίου για ασφαλείς και εύχρηστες συναλλαγές.

Εκτενώς κατά τις προηγούμενες ενότητες έχουν αναφερθεί οι διατάξεις, οι οποίες αφορούν τις ηλεκτρονικές υπογραφές. Ο ενωσιακός νομοθέτης, αντιλαμβανόμενος την ταχεία εξέλιξη των μέσων τεχνολογίας, εξακολούθησε να υιοθετεί την υβριδική προσέγγιση σε ό,τι αφορά τις ηλεκτρονικές υπογραφές. Την ίδια στιγμή δηλαδή που διατηρεί μία ανοιχτή προσέγγιση ως προς τα χρησιμοποιούμενα τεχνολογικά μέσα, θέτει αυστηρότατες προϋποθέσεις για τις εγκεκριμένες ηλεκτρονικές υπογραφές, τις οποίες αναγνωρίζει ως ισόκυρες των ιδιόγραφων. Επιπλέον, ενώ αναγνωρίζει τρεις τύπους ηλεκτρονικών υπογραφών, με τη διατύπωση που υιοθετεί στο άρθρο 25, εν τοις πράγμασι περιορίζει τις κατηγορίες σε δύο, αυτή των απλών ηλεκτρονικών υπογραφών κι εκείνη των εγκεκριμένων.

Επιπροσθέτως, πλέον απαιτεί την υιοθέτηση ενός ελάχιστου επιπέδου διασφάλισης των παρεχόμενων υπηρεσιών σε ό,τι αφορά τα πιστοποιητικά και τα δεδομένα δημιουργίας ηλεκτρονικών υπογραφών. Το δε θεσμικό πλαίσιο για τους παρόχους υπηρεσιών εμπιστοσύνης αυστηροποιείται, όταν πρόκειται εκείνοι να παρέχουν εγκεκριμένες υπηρεσίες εμπιστοσύνης, οι οποίες είναι οι μόνες που επιτρέπουν τη δημιουργία και τη χρήση εγκεκριμένων ηλεκτρονικών υπογραφών. Με αυτό τον τρόπο διατηρεί τις τέσσερις αρχές που η Οδηγία 99/93/Ε.Κ. είχε υιοθετήσεις για τους «έμπιστους τρίτους» φορείς (Παρόχους Υπηρεσιών

[144] Βλ. αιτιολογική σκέψη 2 του Προοιμίου του Κανονισμού (Ε.Ε.) 910/2014: «Επιδίωξη του κανονισμού είναι να ενισχυθεί η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές εντός της εσωτερικής αγοράς, με την παροχή κοινής βάσης για ασφαλείς ηλεκτρονικές αλληλεπιδράσεις μεταξύ των πολιτών, των επιχειρήσεων και των δημόσιων αρχών, αυξάνοντας έτσι την αποτελεσματικότητα των δημόσιων και ιδιωτικών επιγραμμικών υπηρεσιών, του ηλεκτρονικού επιχειρείν και του ηλεκτρονικού εμπορίου στην Ένωση.»

Πιστοποίησης), ενώ ταυτόχρονα ενισχύει το ρυθμιστικό πλαίσιο προστατεύοντας έτι περαιτέρω τα βασιζόμενα μέρη.

4.3. Η προσέγγιση των ηλεκτρονικών υπογραφών από τα ελληνικά πολιτικά δικαστήρια.

Ήδη τόσο κατά την εξέταση των ηλεκτρονικών εγγράφων, αλλά και των κατηγοριών ηλεκτρονικών υπογραφών που αναγνωρίζει ο Κανονισμός (Ε.Ε.) 910/2014 διατυπώθηκαν οι απόψεις που υποστηρίζονται στην ελληνική νομική θεωρία. Στην παρούσα ενότητα επιχειρείται να εξεταστεί η προσέγγιση των ελληνικών πολιτικών δικαστηρίων αναφορικά με την ηλεκτρονική υπογραφή και συνακόλουθα τα έννομα αποτελέσματα που αυτή παράγει σε επίπεδο ουσιαστικού και δικονομικού δικαίου. Θα πρέπει να σημειωθεί ωστόσο, ότι η νομολογία επί του θέματος παρουσιάζει αρκετά μικρό εύρος, ενώ η συντριπτική πλειοψηφία των αποφάσεων αφορά το προϊσχύον θεσμικό πλαίσιο του ΠΔ 150/2001. Ωστόσο, όπως αναπτύχθηκε ήδη, ακόμα και στην περίπτωση του προεδρικού διατάγματος παρατηρούνται οι ίδιες διακρίσεις ηλεκτρονικών υπογραφών, ήτοι οι απλές, οι προηγμένες και τέλος οι αναγνωρισμένες ως ισόκυρες των ιδιόγραφων. Δεδομένου ότι η διαφοροποιήσεις στον Κανονισμό αφορούν την τελευταία κατηγορία, δηλαδή των αναγνωρισμένων ηλεκτρονικών υπογραφών, και δη τις προϋποθέσεις δημιουργίας τους, θα ήταν ασφαλές να προχωρήσουμε στην εξαγωγή συμπερασμάτων αναφορικά με τις έννομες συνέπειες των ηλεκτρονικών υπογραφών, όπως αυτές αντιμετωπίζονται από τον Έλληνα εφαρμοστή του δικαίου.

Για να έχει αποδεικτική δύναμη ένα ηλεκτρονικό έγγραφο θα πρέπει να φέρει την ηλεκτρονική υπογραφή του εκδότη του κατά άρθρα 443 και 444 παρ. 2 ΚΠολΔ, ενώ για να ελεγχθεί το κύρος του ηλεκτρονικού εγγράφου θα πρέπει εξετασθεί ο τύπος (έγγραφος ή μη) της δικαιοπραξίας[145]. Έχει τονιστεί δε κατά το προϊσχύον δίκαιο[146] ότι «οι διατάξεις του π.δ. 150/2001, εισαχθείσες προς εναρμόνιση με το κοινοτικό δίκαιο και λόγω του αντικειμένου τους, είναι εντόνως δημοσίας τάξεως και δεν δύναται να τροποποιηθούν με συμφωνία και δη με τη δικονομική σύμβαση (ημερομηνία επίσκεψης …], η οποία προδήλως δεν αναφέρεται σε κατάργηση των προϋποθέσεων της ηλεκτρονικής υπογραφής, αλλά η δικονομική αυτή συμφωνία προσδίδει αποδεικτική δύναμη ιδιωτικού εγγράφου, στα ένδικα ηλεκτρονικά έγγραφα υπό την αυτονόητη και απαραίτητη προϋπόθεση νόμιμης εκδόσεώς τους πράγμα που σημαίνει ότι αυτά πρέπει να έχουν εξοπλισθεί με την ηλεκτρονική υπογραφή (ημερομηνία επίσκεψης …]». Από τον τρόπο διαπίστωσης δε για την ισχύ των διατάξεων για τις ηλεκτρονικές υπογραφές, αναγκαία συμπεραίνεται ότι το αυτό ισχύει και για το ισχύον δίκαιο.

[145] ΜονΠρΡόδου 841/2012, ΒΝΔ NOMOS
[146] ΕιρΑθηνών 3165/2012, ΑΡΜ 2013 ΑΡΜ 2013 σ. 623,

Εκ των ανωτέρω συνάγεται το συμπέρασμα, αναφορικά με το κύρος των ηλεκτρονικών εγγράφων ότι για τον έλεγχό τους, όπου απαιτείται ιδιόχειρη υπογραφή για τα παραδοσιακά έγγραφα, τότε η μόνη αποδεκτή κατηγορία είναι αυτή της εγκεκριμένης ηλεκτρονικής υπογραφής. Θα πρέπει βέβαια να τονιστεί, ότι, σε κάθε περίπτωση, θα πρέπει να ελέγχονται οι προϋποθέσεις των ουσιαστικών διατάξεων για τη θέση της ιδιόχειρης υπογραφής και να ερμηνεύονται διασταλτικά ανταποκρινόμενες έτσι στα υπάρχοντα τεχνολογικά μέσα.

Περαιτέρω, αναφορικά με την αποδεικτική δύναμη των ηλεκτρονικών, σημειώνεται σε πλειάδα δικαστικών αποφάσεων[147] ότι στις περιπτώσεις που από τα μέρη δεν έχει οριστεί ως απαραίτητη η τήρηση έγγραφου τύπου (άρθρο 160 ΑΚ) αρκεί η απλή ηλεκτρονική υπογραφή. Μάλιστα, υπενθυμίζεται εν προκειμένω ότι επί απλών ηλεκτρονικών υπογραφών για να θεωρηθούν έγκυρες και να προσδώσουν στις μηχανικές απεικονίσεις πλήρη αποδεικτική δύναμη θα πρέπει να αποδεικνύεται ότι αυτή λειτουργεί ως «τελολογικό υποκατάστατο της ιδιόχειρης υπογραφής».[148]

Υπό το φως των ανωτέρω διαπιστώσεων αξίζει να γίνει μία ειδικότερη μνεία στις ειδικότερες μορφές των απλών ηλεκτρονικών υπογραφών που γίνεται δεκτό από τη νομολογία ότι υπό περιστάσεις μπορούν γίνει δεκτό ότι πληρούν τις προϋποθέσεις του άρθρου 445 ΚΠολΔ.

Η πλέον συχνή περίπτωση απλών ηλεκτρονικών υπογραφών αποτελούν η μοναδική για τον κάθε χρήστη διεύθυνση του ηλεκτρονικού ταχυδρομείου.[149] Ειδικότερα, έχει διατυπωθεί η άποψη ότι, για τη λειτουργία του ηλεκτρονικού ταχυδρομείου (e-mail) ως μέσου επικοινωνίας στο διαδίκτυο, απαιτείται σύμφωνα με τα διδάγματα της κοινής πείρας, εκτός της σύνδεσης με κάποιον διαμετακομιστή και η χρήση ενός ειδικού κωδικού, βάσει του οποίου αναγνωρίζεται ο χρήστης στο σύστημα είτε ως αποστολέας είτε ως λήπτης ηλεκτρονικών μηνυμάτων. Ο κωδικός αυτός αποτελεί την ηλεκτρονική διεύθυνση (e-mail) του χρήστη, έτσι όπως αυτή διαμορφώνεται κατά πρωτότυπο τρόπο από τον ίδιο με τη χρήση χαρακτήρων της επιλογής του, οι οποίοι συνδυάζονται με το σύμβολο, και με χαρακτήρες που θέτει ο διαμετακομιστής, κατά τέτοιον τρόπο ώστε ο συγκεκριμένος συνδυασμός χαρακτήρων να αφορά μόνον στον χρήστη που τον έχει ορίσει, χωρίς να είναι δυνατόν να χρησιμοποιηθεί νόμιμα από άλλον. Η απεικόνιση της διεύθυνσης του αποστολέα πάνω στο μήνυμα καθιστά αυτόν απολύτως συγκεκριμένο για τον παραλήπτη, με συνέπεια να μην είναι δυνατόν να επέλθει σύγχυση του με άλλον χρήστη του ίδιου συστήματος, ενώ η ταύτιση του με το περιεχόμενο του μηνύματος είναι άρρηκτη.[150] Αναγνωρίζεται βέβαια, η ύπαρξη κινδύνου, ότι η αποστολή του

[147] ΜονΠρΧαλκίδας 89/2014 Δ/ΝΗ 2015, σ. 251, ΜονΠρΑθηνών 1327/2001, ΔΕΕ 4/2001 με παρατηρήσεις Κοσούλη, σ. 377 = Δ 32 (2001) με παρατηρήσεις Μπέη Κ., ΕιρΑθηνών 3165 /2012 ΑΡΜ 2013, σ. 632
[148] Κ. Δελούκα-Ιγγλέση, ό.π., σ. 213
[149] ΜονΠρΧαλκίδας 89/2014 ό.π., σ. 251, ΜονΠρΑθηνών 1327/2001 ό.π., ΕιρΑθηνών 3165/2012 ό.π.
[150] ΜονΠρΑθηνών 1932/2011 Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ ΝΟΜΟS

συγκεκριμένου μηνύματος έγινε από άλλο πρόσωπο από αυτό στο οποίο ανήκει η συγκεκριμένη ηλεκτρονική διεύθυνση κάνοντας χρήση αυτής (με οποιαδήποτε τρόπο) χωρίς την έγκριση του. Ωστόσο, όπως έχει προταθεί[151] «η ελαττωματικότητα αυτή του μηνύματος που εστάλη, παραπέμπει ευθέως στις διατάξεις περί πλαστότητας του ΚΠολΔ (460 επ.) εγκαθιστώντας αναστροφή του βάρους απόδειξης στον επικαλούμενο αυτή, για το λόγο ότι η λειτουργία του συστήματος του ηλεκτρονικού ταχυδρομείου παρέχει εγγυήσεις για την πιστότητα της και η οποιαδήποτε παθολογία εμφανίζεται δεν προέρχεται από ελάττωμα του συστήματος αλλά από επέμβαση τρίτου σε αυτό, γεγονός το οποίο δεν ανήκει στη σφαίρα επιρροής του φερόμενου ως αποστολέα. Με δεδομένα τα ανωτέρω περιορίζεται ουσιαστικά η ενέργεια της § 4 του άρθρου 457 του ΚΠολΔ στο ζήτημα της ταυτότητας μεταξύ περιεχομένου του σκληρού δίσκου του ηλεκτρονικού υπολογιστή και της μηχανικής απεικόνισης τους»

Ιδιαίτερης αναφοράς για την περίπτωση αναγνώρισης των απλών ηλεκτρονικών υπογραφών χρήζει η περίπτωση του μοναδικού αριθμού του αποστολέα SMS (Short Message Message), η οποία οδήγησε το Μονομελές Πρωτοδικείου Ηρακλείου[152] στη διαπίστωση ότι και σε αυτή την περίπτωση πρόκειται για ηλεκτρονικό έγγραφο, το οποίο έχει πλήρη αποδεικτική δύναμη. Ειδικότερα, δεχόμενο το δικαστήριο ότι τα κινητά τηλέφωνα λειτουργούν με τον ίδιο τρόπο, όπως οι Η/Υ, οδηγείται στο συμπέρασμα ότι τα sms συνιστούν ηλεκτρονικό έγγραφο και δη μηχανική απεικόνιση κατά τα οριζόμενα του άρθρου 444 παρ. 1 ΚΠολΔ. Περαιτέρω, γίνεται δεκτό ότι «το γραπτό μήνυμα, άλλως Short Message Service γνωστό και ως SMS, είναι υπηρεσία της κινητής τηλεφωνίας, με την οποία ο χρήστης έχει τη δυνατότητα να αποστείλει ή να παραλάβει σύντομο γραπτό μήνυμα από άλλους χρήστες, στην οθόνη του κινητού του τηλεφώνου.». Αναφορικά δε με την υπογραφή ως τρόπο ταυτοποίησης του αποστολέα του μηνύματος δέχεται το δικαστήριο ότι «ο εκάστοτε συντάκτης όμως των συγκεκριμένων εγγράφων (sms) αποδέχεται και επιδιώκει να καταγραφούν αυτά με σταθερό τρόπο σε κάποια από τις "μακροπρόθεσμες" μνήμες του κινητού τηλεφώνου του παραλήπτη (σκληρός δίσκος ή μνήμη SIM), ώστε ο τελευταίος, όχι μόνο να προβεί στην άπαξ προβολή αυτών και να λάβει έτσι γνώση του περιεχομένου τους, αλλά επιπροσθέτως, να δύναται στο μέλλον και σε κάθε στιγμή να τα ανασύρει, ώστε να τα αναγνώσει ξανά, καθιστάμενος διαρκής κάτοχος του ηλεκτρονικού εγγράφου. Η δυνατότητα δε αυτή που παρέχεται στον παραλήπτη του sms τελεί σε γνώση του αποστολέα, αφού και ο τελευταίος με τον ίδιο τρόπο πράττει. Πρέπει να γίνει δεκτό, συνεπώς, ότι υπάρχει τεκμαιρόμενη συναίνεση του αποστολέα να καταστήσει τον παραλήπτη κοινωνό και άρα νόμιμο κάτοχο του μηνύματος sms. Δικονομικά δε, τα γραπτά μηνύματα θα πρέπει να αντιμετωπιστούν για την ταυτότητα του νομικού λόγου, όπως οι επιστολές, αφού σε αμφότερες τις μορφές αυτού του είδους της επικοινωνίας συνυπάρχουν τα

[151] ΜονΠρΠειραιά 2150/2017 Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ NOMOS
[152] ΜονΠρΗρακλείου 1085/2018 Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ NOMOS

στοιχεία της αποτυπωμένης σε αναγνώσιμη μορφή επικοινωνίας από απόσταση, ενώ η μετάβαση από την κυριαρχία της επιστολής στην κυριαρχία του sms, έγινε κυρίως λόγω του εκσυγχρονισμού της διαθέσιμης τεχνολογίας.». Εν προκειμένω δηλαδή αναγνωρίζεται ότι απλά για τη γνωστοποίηση της βούλησης του αποστολέα μηνύματος (ηλεκτρονικού εγγράφου), εφόσον δεν απαιτείται κάποιες από τις προϋποθέσεις του άρθρου 160 ΑΚ είναι αρκετή η διαπίστωση της ταυτότητας του αποστολέα. Ως εκ τούτου, λαμβανομένων υπ' όψιν των υπό κρίση περιστάσεων, κρίθηκε ότι ο μοναδικός αριθμός κινητού τηλεφώνου του χρήστη μπορεί να λειτουργήσει ως απλή ηλεκτρονική υπογραφή, η οποία λειτουργεί τελολογικά ως υποκατάστατο της ιδιόχειρης υπογραφής.

Συμπερασματικά, λαμβάνοντας κανείς υπ' όψιν του τη θέσης της νομολογίας για το τι δέχεται ως υπογεγραμμένο ηλεκτρονικό έγγραφο, επανέρχεται στις αρχικές θεωρητικές διαπιστώσεις για τις έννομες συνέπειες των κατηγοριών των ηλεκτρονικών υπογραφών. Ειδικότερα, σε ό,τι αφορά τις εγκεκριμένες ηλεκτρονικές υπογραφές (αναγνωρισμένες κατά το προϊσχύον δίκαιο), αυτές αναγνωρίζονται ως οι μόνες ισόκυρες των ιδιόγραφων παράγοντας όλες τις έννομες συνέπειες τόσο στο ουσιαστικό αστικό δίκαιο (άρθρο 160 ΑΚ), όσο και στο δικονομικό (άρθρο 445 ΚΠολΔ).

Ωστόσο, ιδιαίτερης μνείας θα πρέπει να τύχουν οι απλές ηλεκτρονικές υπογραφές σε ό,τι αφορά το δίκαιο απόδειξης στην Πολιτική Δικονομία. Ειδικότερα, γίνεται αντιληπτό ότι, σε περιπτώσεις που δεν απαιτείται ιδιαίτερος έγγραφος τύπος, εκείνες είναι σε θέση (υπό τις προαναφερθείσες προϋποθέσεις) να θεωρηθούν ισόκυρες των ιδιόγραφων και να πληρούν τις προϋποθέσεις του άρθρου 445 ΚΠολΔ. Παρατηρείται όμως η τάση της ελληνικής νομολογίας να περιορίζεται αποκλειστικά στη λειτουργία των απλών ηλεκτρονικών υπογραφών ως διαπιστεύσεων της ταυτότητας του συντάκτη του ηλεκτρονικού εγγράφου – μηνύματος, αδιαφορώντας για τις υπόλοιπες τρείς λειτουργίες που πρέπει να επιτελούν οι ηλεκτρονικές υπογραφές. Με αυτό τον τρόπο ωστόσο ελλοχεύει ο κίνδυνος ανασφάλειας στις ηλεκτρονικές συναλλαγές και συνδιαλλαγές. Η διασταλτική ερμηνεία που εφαρμόζουν τα ελληνικά δικαστήρια αναφορικά με τις απλές ηλεκτρονικές συναλλαγές δεν παρέχει τις δέουσες εγγυήσεις στις οποίες αποσκοπούσε το π.δ. 150/2001 και πλέον ο Κανονισμός για τις ηλεκτρονικές συναλλαγές. Θα πρέπει να επιδειχθεί η μέγιστη πρόνοια, ώστε η αξιοποίηση των περιθωρίων που επιτρέπει το άρθρο 26 του Κανονισμού για την κρίση των εθνικών δικαστηρίων, να μην καταλήξει σε καταστρατήγηση των διατάξεων που έχουν ταχθεί για την καθιέρωση ενός ασφαλούς περιβάλλοντος διαδικτυακής αλληλεπίδρασης.

Συμπεράσματα

Στην παρούσα διπλωματική εργασία επιχειρήθηκε να αναλυθούν τα βασικότερα νομικά ζητήματα που άπτονται των ηλεκτρονικών υπογραφών. Δια τούτο επιχειρήθηκε, όχι μόνο η ανάπτυξη της φύσης και των κατηγοριών τους υπό τις κρατούσες νομικές (και τεχνολογικές συνθήκες), αλλά πολύ περισσότερο η λειτουργίες που αυτές καλούνται να επιτελέσουν.

Όπως έχει ήδη αναφερθεί, ο όρος «ηλεκτρονική υπογραφή» συνιστά έναν αμιγώς νομικό όρο, ο οποίος αναφέρεται στη διαδικασία τεκμηρίωσης, όχι μόνο της ταυτότητας του υπογράφοντα, αλλά και του αναλλοίωτου των ηλεκτρονικών εγγράφων. Τα τελευταία, με την ηλεκτρονική υπογραφή, δεν καθίστανται μόνον έγκυρα, αλλά πολύ περισσότερο διαβεβαιώνεται το αναλλοίωτο του περιεχομένου τους, ήτοι δεν μπορούν να υπάρξουν επεμβάσεις σε αυτά, ενώ φέρουν αποκρυσταλλωμένη τη βούληση του συντάκτη τους.

Από τη μέχρι τώρα ανάπτυξη, κατέστη σαφές ότι η τεχνολογία αποτελεί πλέον σημαντικό και αναπόσπαστο μέρος του δικαίου για τις ηλεκτρονικές υπογραφές. Κοινός τόπος αποτελεί η πρωτοπορία της τεχνολογίας και η μεταγενέστερη προσαρμογή των κανόνων δικαίου προς τη νέα πραγματικότητα. Όπως διαπιστώθηκε όμως, ο ενωσιακός νομοθέτης ακολουθώντας την προσέγγιση που εισήχθη ήδη με την Οδηγία 99/93/ΕΚ, με τη θέσπιση του Κανονισμού 910/2014 κατόρθωσε να συμπεριλάβει τα νέα τεχνολογικά επιτεύγματα. Έτσι, τόσο για τα ηλεκτρονικά έγγραφα, όσο και για τις ηλεκτρονικές υπογραφές υιοθετήθηκε επιτυχώς τεχνολογικά ουδέτερη ορολογία. Επιπροσθέτως, η προσέγγιση διπλής διαβάθμισης (two tier approach) παρέχει τη δυνατότητα, από τη μία να παρέχεται ex lege υψηλή δικαιϊκή ασφάλεια, ενώ ταυτόχρονα να επιτρέπεται η αναγνώριση και χαμηλού επιπέδου ηλεκτρονικών υπογραφών, ως ικανών να παράγουν έννομα αποτελέσματα.

Επισημάνθηκε δε, ότι τα ρυθμιζόμενα ηλεκτρονικά έγγραφα που φέρουν την εγκεκριμένη ηλεκτρονική υπογραφή του εκδότη τους συνιστούν την ex lege κατά τον Κανονισμό 910/2014 πλέον αξιόπιστη λύση για την πιστοποίηση της γνησιότητας και του αναλλοίωτου του περιεχομένου τους σε ανοιχτά δίκτυα. Ο Κανονισμός, όπως προαναφέρθηκε, κατόρθωσε να επιλύσει μείζονα προβλήματα, τα οποία είχαν επισημανθεί κατά το προϊσχύον θεσμικό πλαίσιο. Μέσω της αναβάθμισης των υπηρεσιών εμπιστοσύνης σε εγκεκριμένες, ο Κανονισμός (Ε.Ε.) 910/2014 συμβάλει ριζικά στην επίτευξη του ανωτέρω στόχου. Έχοντας μάλιστα θέσει τις ελάχιστες τεχνικές προδιαγραφές κατά την παροχή των τελευταίων καθιστά τις παρεχόμενες υπηρεσίες ποιοτικά συγκρίσιμες σε όλη την Ένωση. Ταυτόχρονα, αυστηροποιώντας τον έλεγχο των εγκεκριμένων παρόχων των υπηρεσιών αυτών, δόθηκε η αναγκαία ώθηση ώστε να διασφαλιστεί η αναγκαία διαλειτουργικότητα των παρεχόμενων προϊόντων εγκεκριμένων ηλεκτρονικών υπογραφών και των εγκεκριμένων υπηρεσιών εμπιστοσύνης.

Ωστόσο, η απόκτηση προηγμένης ή και εγκεκριμένης ηλεκτρονικής υπογραφής οδηγεί σε ένα εύλογο κόστος, το οποίο δεν είναι διατεθειμένος να επωμιστεί ο μέσος κοινωνός του διαδικτύου. Έτσι, παρατηρείται η προτίμηση των απλών ηλεκτρονικών υπογραφών για τις περιπτώσεις που δεν απαιτείται η τήρηση έγγραφου τύπου, δια των οποίων απλώς πιστοποιείται η ταυτότητα του συντάσσοντος το ηλεκτρονικό μήνυμα. Στις περιπτώσεις αυτές το βάρος να διαγνωσθεί εάν η ηλεκτρονική υπογραφή πληροί όλες τις απαραίτητες προϋποθέσεις για το κύρος της δικαιοπραξίας και για την αποδεικτική δύναμη του εγγράφου μετατοπίζεται στον εθνικό δικαστή. Και μολονότι έχει παρατηρηθεί ότι σε μεγάλο βαθμό η συμμόρφωση των ελληνικών δικαστηρίων με τις στοχεύσεις του Κανονισμού 910/2014, θα πρέπει να σημειωθεί ότι η προσέγγιση της κάθε περίπτωσης θα πρέπει να γίνεται ad hoc και με ιδιαίτερη προσοχή, προκειμένου να μην τίθεται εν αμφιβόλω η ασφάλεια δικαίου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ελληνική Βιβλιογραφία

- Αγγελάκης Αντώνιος, Η προαναγγελθείσα επανάσταση: τεχνολογική αλλαγή και προεκτάσεις υπό το πρίσμα της «4ης Βιομηχανικής Εποχής» Μέρος Ι - Θεωρητική επισκόπηση, Ερευνητικά Κείμενα ΙΜΕ ΓΣΕΒΕΕ, 6/2019, σ. 64, διαθέσιμο στην ιστοσελίδα https://imegsevee.gr/wp-content/uploads/2019/10/4%CE%B7-CE%B2%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%B5%CF%80%CE%B1%CE%BD%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7_%CE%BC1.pdf (ημερομηνία πρόσβασης: 28-05-2020)

- Γώγος Κωνσταντίνος, Η ανυπόστατη διοικητική πράξη, εκδόσεις Σάκκουλας Αθήνα-Θεσσαλονίκη, 2012

- Δελούκα-Ιγγλέση Κορνηλία, Νομικά Θέματα Ηλεκτρονικού Εμπορίου. 2η έκδ. εκδόσεις Σάκκουλας, Αθήνα Θεσσαλονίκη, 2015

- Ζέκος Γ., Διαδίκτυο, Η/Υ & τηλεπικοινωνίες στο ελληνικό δίκαιο, Εκδόσεις Σάκκουλας, Αθήνα-Θεσσαλονίκη 2017

- Ιγγλεζάκης Ι., Δίκαιο πληροφορικής, 3η έκδ., εκδόσεις Αθήνα-Θεσσαλονίκη 2018

- Καραγιάννης Β., Το κοινοτικό νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές - Η Οδηγία 1999/93/ΕΚ. ΔΕΕ 6/2000, σ. 580 επ.

- Καραδημητρίου Α. Κοσμάς, Η Ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο, Μη εκδοθείσα Διδακτορική Διατριβή 2007, Αριστοτέλειο Πανεπιστήμιο

- Καράκωστας, Γ., Δίκαιο και Internet: νομικά ζητήματα του διαδικτύου. 2η έκδοση. Αθήνα, Π.Ν. Σάκκουλας Θεσσαλονίκης 2003

- Καρέκλης Α. Πέτρος, Επιπτώσεις του Internet στη λειτουργία και κερδοφορία των επιχειρήσεων-Οφέλη από τη χρήση Υπηρεσιών ηλεκτρονικής τραπεζικής, Δελτίον Ένωσης Ελληνικών Τραπεζών Ιούλιος-Αύγουστος-Σεπτέμβριος 2003 σ. 41/ διαθέσιμο στην ηλεκτρονική διεύθυνση https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/3_2003.pdf (ημερομηνία επίσκεψης 03-04-2020)

- Κόμνιος Κομνηνός, Το νέο ευρωπαϊκό νομοθετικό πλαίσιο για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης - Συναφή ζητήματα δικαίου απόδειξης, Εφαρμογές Αστικού Δικαίου & Πολιτικής Δικονομίας 6 (2017), σ. 498-510.

- Κοσούλης Κ. (2001), Η αποδεικτική δύναμη του e-mail, σχόλιο στην απόφαση ΜονΠρΑθηνών 1327/2001, ΔΕΕ (4) 2001

- Κουμεντάκης Σταύρος, «Η 4η Βιομηχανική Επανάσταση - Ρυθμίζεται, άραγε, η ανάπτυξη;», Capital.gr, 03-10-2019 διαθέσιμο στην ιστοσελίδα https://www.capital.gr/arthra/3385609/i-4i-biomixaniki-epanastasi-ruthmizetai-arage-i-anaptuxi (ημερομηνία προσπέλασης: 28-05-2020)

- Λιναρίτης Ι.. Η νομοθετική ρύθμιση των ηλεκτρονικών υπογραφών μετά την ενσωμάτωση της Οδηγίας 99/93 της ΕΕ στο ελληνικό δίκαιο με το ΠΔ 150/2001, ΔΕΕ. 3/2002, σ. 257.

- Μανιώτης, Δ., Η ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων στο αστικό δικονομικό δίκαιο. Αντ. Σάκκουλας. Αθήνα-Κομοτηνή 1999

- Μητρακάς Α., Οι ηλεκτρονικές υπογραφές στο ευρωπαϊκό και ελληνικό δίκαιο: Ζητήματα εφαρμογών στον τραπεζικό τομέα. Δελτίο ΕΕΤ εξάμηνο 2003, διαθέσιμο στην ηλεκτρονική διεύθυνση https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/3_2003.pdf (ημερομηνία επίσκεψης 03-04-2020)

- Μητσόπουλου Γ./Κεραμέως Κ., Το τηλετύπημα (TELEX) αποτελεί αρχή εγγράφου αποδείξεως υπέρ του αποστολέα του, ΝοΒ 31 (1983), σελ. 330-331

- Μιχαηλίδου Χρυσούλα, Το πρόβλημα της ηλεκτρονικής υπογραφής. Δ. 2000 διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=1479&mnu=3&id=18381 (ημερομηνία επίσκεψης 16-03-2020)

- Παπαθωμά Μπέτγκε Α., «Ηλεκτρονικό εμπόριο: Νομικά ζητήματα κατά τη σύναψη εμπορικών συμβάσεων στο Ίντερνετ», ΔΕΕ 12/1999, σ. 1237

- Σιούλης Χ., Η ευρωπαϊκή νομοθεσία για τις ηλεκτρονικές υπογραφές (Ανάλυση και Σχολιασμός), 2003 διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ebusinessforum.gr/content/downloads/El-Sign_Directive2.pdf (ημερομηνία επίσκεψης 10-02-2020)

- Υπουργείο Εθνικής Παιδείας και Θρησκευμάτων – Παιδαγωγικό Ινστιτούτο (1999) «Τεχνολογία Υπολογιστικών Συστημάτων & Λειτουργικά Συστήματα», Αθήνα, Οργανισμός

Εκδόσεως Διδακτικών Βιβλίων Ανακτήθηκε , διαθέσιμο στην ηλεκτρονική διεύθυνση http://ebooks.edu.gr/modules/ebook/show.php/DSB103/173/1204,4404/ (ημερομηνία επίσκεψης 18-01-2018)

- Φιλιππoπούλου, Ε.(200).Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου. ΔΕΕ 11/2000,σ. 1086.

- Χριστοδούλου Κωνσταντίνος (2000) «Τρία νέα ζητήματα του δικαίου των ηλεκτρονικών εγγράφων μετά το σχέδιο νόμου ηλεκτρονικές υπογραφές» Δ. 2000. , διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=&mnu=0&id=18351 (ημερομηνία επίσκεψης 10-05-2019)

Του ίδιου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία. Αθήνα-Κομοτηνή, Αντ. Ν Σάκκουλας 2001

Του ίδιου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία μετά τις νέες κοινοτικές ρυθμίσεις . 2η έκδοση. Αθήνα-Κομοτηνή: Αντ. Ν. Σάκκουλας 2004

Του ίδιου (2013). Επιτομή Ηλεκτρονικού Αστικού Δικαίου, δεύτερη έκδοση. Αθήνα-Κομοτηνή: Αντ. Σάκκουλας

2. Νομολογία

- ΑΠ 2064/2006, διαθέσιμη στην ηλεκτρονική διεύθυνση http://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=ANLZk4H2orJ2n0j0ScCC85opHq7NQD&apof=2064_2006&info=%D0%CF%CB%C9%D4%C9%CA%C5%D3%20-%20%20%C21

- ΑΠ 3/2001, Δ. 2001, με ενημ. σημ. Κ.Ε.Μ. διαθέσιμο στην ηλεκτρονική σελίδα http://www.kostasbeys.gr/articles.php?s=5&mid=&mnu=0&id=18031&keyw=%C1%D0+3%2F2001&sr=search&pg= (τελευταία επίσκεψη 10-04-2020)

- ΕφΑθηνών 46/2014 ΔΕΕ 4/2014, σ. 373

- ΕφΑθηνών 32/2011, ΔΕΕ 5/2011 σ. 591

- ΕφΠατρων 143/2008, ΕπισκΕΔ 2008, σ. 571

- ΜονΠρΗρακλείου 1085/2018 Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ NOMOS

- ΜονΠρΠειραιά 2150/2017 Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ NOMOS

- ΜονΠρΧαλκιδας 89/2014 .Δ/ΝΗ 2015, σ. 251
- ΜονΠρΡόδου 841/2012 Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ NOMOS
- ΜονΠρΑθηνών 1932/2011. Α ΔΗΜΟΣΙΕΥΣΗ ΒΝΔ NOMOS
- ΜονΠρΑθηνών 1963/2004, Δ. Μάιος 2005 με παρατηρήσεις Μπέη Κ., 2005, διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.kostasbeys.gr/articles.php?s=5&mid=&mnu=0&id=21305&keyw=%CC%D0%F1%C1%E8+1963%2F2004&sr=search&pg= (ημερομηνία επίσκεψης 20-05-2019)
- ΜονΠρΑθ 1327/2001, ΔΕΕ 4/2001 με παρατηρήσεις Κοσούλη,σ. 377 = Δ 32 (2001) με παρατηρήσεις Μπέη Κ, Σ. 457
- ΕιρΑθηνών 3165/2012 ΑΡΜ 2013, σ. 632

3. Ξενόγλωσση βιβλιογραφία

- Andress J. (2014) The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition. Oxford: Elsevier Inc.
- Bernard Marr, “What is Industry 4.0? Here's A Super Easy Explanation For Anyone”, Forbes 02-09-2018, διαθέσιμο στην ηλεκτρονική διεύθυνση https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#1a5b52999788 (ημερομηνία προσπέλασης: 28-05-2020).
- Bose S. and Vijayakumar P. (2016) Cryptography and Network Security. Chennai: Pearson India Education Services Pvt.
- Choudhury, S (Ed.). (2002) Public Key Infrastructure Implementation and Design. New York: D. M&T Books.

4. Άλλα έγγραφα:

- Επιτροπή των Ευρωπαϊκών Κοινοτήτων (2006).COM(2006). Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Έκθεση αναφορικά με τη λειτουργία της οδηγίας 1999/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. διαθέσιμο στην ηλεκτρονική διεύθυνση:

- https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120: FIN:EL:PDF (ημερομηνία επίσκεψης 02-05-2020)
- Ανακοίνωση της Επιτροπής της 26ης Αυγούστου 2010 με τίτλο «Ψηφιακό θεματολόγιο για την Ευρώπη» διαθέσιμο στην ηλεκτρονική διεύθυνση https://ec.europa.eu/commission/presscorner/detail/el/MEMO_10_200 (ημερομηνία επίσκεψης 23-05-2020)

5. Ηλεκτρονικές διευθύνσεις:

- Άρειος Πάγος: http://www.areiospagos.gr
- Βάσεις Νομικών Δεδομένων NOMOS: https://lawdb.intrasoftnet.com/
- Ένωση Ελληνικών Τραπεζών: https://www.hba.gr
- Ευρωπαϊκή Επιτροπή: https://eur-lex.europa.eu
- Ινστιτούτο Μικρών Επιχειρήσεων ΓΣΕΒΕΕ: https://imegsevee.gr/
- Κέντρο Δικανικών Μελετών Αθήνας – Κώστας Μπέης: http://www.kostasbeys.gr
- Οργανισμός Εκδόσεως Διδακτικών Βιβλίων: http://ebooks.edu.gr
- E-Business Forum: http://www.ebusinessforum.gr
- Eur-LEX: https://eur-lex.europa.eu
- Capital.gr (ηλεκτρονικός οικονομικός τύπος): https://www.capital.gr
- Forbes (ηλεκτρονικός οικονομικός τύπος): https://www.forbes.com