ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΝΟΜΙΚΗΣ

ΑΚΑΔΗΜΑΙΚΟ ΈΤΟΣ: 2021-2022

ΚΑΤΕΥΘΥΝΣΗ: ΕΥΡΩΠΑΙΚΟ ΕΜΠΟΡΙΚΟ ΔΙΚΑΙΟ

Μεταπτυχιακή Διπλωματική Εργασία

«Οι επερχόμενες αλλαγές μετά την πρόταση της Ευρωπαϊκής Επιτροπής για αναθεώρηση της Οδηγίας NIS, Το υπό διαμόρφωση νομοθετικό πλαίσιο του κυβερνοχώρου»

Της Σόνιας Τσαχίδου

ΕΠΙΒΛΕΠΟΥΣΑ: Δρ Χαρίκλεια Βλάχου

ΣΥΝΑΞΙΟΛΟΓΗΤΗΣ: Δρ Μιχάλης Χατζηπαναγιώτης

ΗΜΕΡΟΜΗΝΙΑ ΠΑΡΑΔΟΣΗΣ: 8/12/2021

Περιεχόμενα

Εισαγωγή

Την τελευταία δεκαετία υπήρξε ραγδαία πρόοδος της ανθρωπότητας, σημαντική αύξηση της παραγωγικότητας, κρίσιμα επιτεύγματα στο πεδίο της καινοτομίας, ιδίως λόγω της ραγδαίας ανάπτυξης των τεχνολογιών πληροφορικής και επικοινωνίας.[1] Ως τεχνολογίες πληροφορικής και επικοινωνίας θεωρούνται *«τα ολοκληρωμένα συστήματα δικτύων, τα οποία είναι διασυνδεδεμένα μεταξύ τους και επιτρέπουν την ροή πληροφοριακών δεδομένων»*.[2] Η έλευση αυτών των νέων τεχνολογιών στην καθημερινότητα της κοινωνίας επέφερε αξιοσημείωτες αλλαγές ιδίως στους τομείς που σχετίζονται με την ενέργεια, τις μεταφορές, τις επικοινωνίες και τα χρηματοοικονομικά.[3] Περαιτέρω, μέσω των εν λόγω τεχνολογιών ενισχύθηκε και η δημόσια διοίκηση, η δημόσια υγεία, η εκπαίδευση και η εθνική ασφάλεια.[4] Η σύνδεση της ανθρωπότητας με αυτές τις τεχνολογίες πληροφορικής και επικοινωνίας δημιούργησαν ένα χώρο δράσης και επικοινωνίας γνωστό πλέον και ως κυβερνόχωρο.[5] Η έννοια του κυβερνοχώρου είναι μια πρόσφατη και διαφιλονικούμενη έννοια.[6] Είναι σαφώς δύσκολος ο ακριβής προσδιορισμός του. Θα μπορούσε να χαρακτηριστεί ως *«το παγκόσμιο πληροφοριακό περιβάλλον, το οποίο δημιουργείται από τη διασύνδεση αυτοματοποιημένων πληροφοριακών συστημάτων».*[7]

---

[1] Κοσμάς Πιπύρος, Λίλιαν Μήτρου, «Κυβερνοεπίθεση ή κυβερνοπόλεμος;», *Νομική Βιβλιοθήκη*, ΔΙΤΕ (π. ΔΙΜΕΕ), Τεύχος 2/2018, 2018, σελ. 192.

[2] Ibid 1, σελ.192.

[3] Ibid *supra* 1, σελ. 192.

[4] Ibid supra 1, σελ. 192.

[5] Ibid supra 1, σελ.192.

[6] Dimitra Stefanoudi «The Relevance and Applicability of Cybersecurity Laws with Regard to Data Storage on Board Satellites and on the Ground», *Air and Space Law*, Volume 44, Issue 4/5, 2019, pp. 425 – 428.

[7] Ibid supra 1, σελ. 192.

Πρόκειται στην πραγματικότητα για έναν εικονικό χώρο, ο οποίος χαρακτηρίζεται ως ιδιαίτερα ευάλωτος και εύθραυστος λόγω των *«αόρατων επιθέσεων»*, γνωστών και ως κυβερνοεπιθέσεων.[8]

Οι κυβερνοεπιθέσεις αποτελούν τις κακόβουλες ενέργειες κατά των ως άνω πληροφοριακών συστημάτων.[9] Συνήθως, οι εν λόγω επιθέσεις στρέφονται κατά των «*κρίσιμων υποδομών*», δηλαδή κατά των πληροφοριακών συστημάτων υψίστης ζωτικής σημασίας ενός κράτους που είναι άμεσα συνδεδεμένα με τη διακυβέρνηση μιας χώρας.[10] Επί παραδείγματι, επιθέσεις κατά του δικτύου ηλεκτρικής ενέργειας, των δημόσιων παροχών νερού ή και του ελέγχου της εναέριας κυκλοφορίας.[11] Συνεπώς, μια κυβερνοεπίθεση δύναται να συμβάλει στην κατάρρευση ενός κράτους, καθώς οι εν λόγω υποδομές ορισμένες φορές είναι σε αλληλεξάρτηση με άλλες υποδομές ένας κράτους.[12] Κατ' επέκταση θα μπορούσε να αναφερθεί ότι ο κεντρικός στόχος των κυβερνοεπιθέσεων είναι η καταστροφή των δικτύων αυτών με τη διακοπή των υπηρεσιών που παρέχουν σε ένα κράτος ή και η νόθευση των δεδομένων που υφίστανται στις εν λόγω υπηρεσίες με σκοπό τον έλεγχο, την εκμετάλλευση και την υπονόμευση της διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας.[13]

Η αντιμετώπιση των ως άνω προκλήσεων, οι οποίες ξεπερνούν τα εθνικά σύνορα ενός κράτους, είναι δύσκολο να επιτευχθεί ικανοποιητικά σε εθνικό επίπεδο. Το 2013 η Ευρωπαϊκή Επιτροπή και ο Ύπατος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας ανακοίνωσαν ότι η ασφάλεια και η

[8] Ibid supra 1, σελ. 192.

[9] Ibid supra 1, σελ. 192.

[10] Ibid supra 1, σελ. 192.

[11] Leandros Maglaras, George Drivas, Kleanthis Noou, Stylianos Rallis, «NIS directive: The case of Greece», *EAI Endorsed Transactions on Security and Safety*, Vol 4, Issue 14 , 2018, pp 1.

[12] Ibid 11, pp. 1.

[13] Ibid supra 1, σελ. 192.

αξιοπιστία του κυβερνοχώρου αποτελεί άμεση προτεραιότητα της Ευρωπαϊκής Ένωσης (εφεξής Ένωση).[14] Ο κύριος σκοπός της πρότασης της Ένωσης είναι η «*θωράκιση της Ευρώπης από εξωτερικές απειλές»* και η διασφάλιση ενός ασφαλούς ψηφιακού περιβάλλοντος.[15] Το μέγεθος των κινδύνων φαίνεται ότι είχε υποτιμηθεί λόγω της ελλιπούς καταγραφής των περιστατικών κυβερνοεπίθεσης που κοινοποιούνταν στις αρμόδιες αρχές σε σχέση με τα πραγματικά περιστατικά που λάμβαναν χώρα στην Ένωση.[16] Οι επιχειρήσεις που δέχονταν επιθέσεις φοβόντουσαν να τις κοινοποιήσουν λόγω του ενδεχόμενου πλήγματος της φήμης και αξιοπιστίας τους προς τους πελάτες τους.[17] Η εν λόγω πρόταση στοχεύει στην ενημέρωση του κοινού με απώτερο σκοπό την εξάλειψη του ψηφιακού «αναλφαβητισμού».[18] Η προστασία του κυβερνοχώρου δεν αποτελεί ευθύνη μόνο των κρατών άλλα και των πολιτών, οι οποίοι θα πρέπει να ενημερώνονται για το ψηφιακό περιβάλλον ώστε να λαμβάνουν τα απαραίτητα προστατευτικά μέτρα.[19]

Έτσι έπειτα από τρία χρόνια διαπραγματεύσεων οδηγηθήκαμε στην Οδηγία NIS για την ασφάλεια του κυβερνοχώρου της οποίας κύριος στόχος είναι η δημιουργία ένας υψηλού κοινού επίπεδου ασφάλειας των συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.[20] Εντούτοις, το 2020, ήτοι δύο χρόνια μετά

[14] Dimitra Markopoulou, Vangelis Papakonstantinou, Paul de Hert «The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation», *Computer law & security review*, Vol. 35, Issue 6, 2019, pp. 1-2.

[15] Ibid supra 11, pp 4.

[16] Ε. Βαγενά, «Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος», *Νομική Βιβλιοθήκη,* ΔΙΤΕ (π. ΔΙΜΕΕ) , Τεύχος 1/2017, 2017, σελ. 18.

[17] Ibid 16.

[18] Alina Popescu, «The right to information and cybersecurity», *Journal of Law and Public Administration*, Vol. 3, No. 6, 2017, pp. 106.

[19] Ibid 18, pp. 106.

[20] Maria There Holzieitner, Johannes Reichl, «Legal Problems for the Protection of Smart Grids from Cyber Threats», *European Energy Journal*, Vol. 6, Issue 3, 2016, pp. 53-55.

την υιοθέτηση της Οδηγίας NIS, η Επιτροπή και ο Ύπατος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας ανακοίνωσαν εκ νέου τη νέα στρατηγική της Ένωσης για διαμόρφωση ενός ψηφιακού μέλλοντος της Ένωσης για συλλογική ανθεκτικότητα και αυτονομία έναντι των κυβερνοαπειλών.[21] Στις 16 Φεβρουαρίου 2020 η Ευρωπαϊκή Επιτροπή υπέβαλε πρόταση για αναθεώρηση της οδηγίας NIS.[22] Στην αιτιολογική της πρόταση αναφέρεται στην αναγκαιότητα τροποποίησης της υφιστάμενης οδηγίας και θέσπισης μιας νέας ρύθμισης που θα προβλέπει έναν καθολικό και αποτελεσματικό μηχανισμό συνεργασίας στον κυβερνοχώρο.[23]

Σκοπός της παρούσας διπλωματικής εργασίας είναι κατ' αρχάς η μελέτη των εγγενών αδυναμιών της Οδηγία NIS να επιφέρει ένα ομοιόμορφο και καθολικό αποτέλεσμα κατά την εφαρμογή της από τα κράτη μέλη (Ι), οι οποίες οφείλονται ιδίως στην ευρεία διακριτική ευχέρεια που παραχωρήθηκε στα κράτη μέλη κατά την εναρμόνιση και λόγω ασαφειών που διατυπώνονται στο κείμενο της. Οι εν λόγω ασάφειες εξηγούν και την μη αποτελεσματική συνύπαρξη της με τον Κανονισμό GDPR.[24] Ως εκ τούτου, το επόμενο ζήτημα προς εξέταση είναι η έλλειψη σαφούς αναφοράς και οριοθέτησης της σχέσης της οδηγίας με τον Κανονισμό GDPR που οδήγησε την αντιμετώπιση των περιστατικών έλλειψης συνεργασίας μεταξύ των

[21] Ευρωπαϊκή Επιτροπή, Αντιπροσωπεία στην Ελλάδα «Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων». Πρόσβαση 1/10/2021 https://ec.europa.eu/greece/news/20201216____5_el

[22] Πρόταση Ευρωπαϊκής Επιτροπής «Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148», ημερομηνίας 16/12/2020.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52020PC0823

[23] Ibid 22 (Βλ. Αιτιολογική Έκθεση).

[24] Sandra Schmitz-Berndt, Fabian Anheier, «Synergies in Cybersecurity Incident Reporting - The NIS Cooperation Group Publication 04/20 in Context», *European Data Protection Law Review*, 2021, Vol. 7 Issue 1, p101.

εμπλεκόμενων μερών και ανταλλαγή των πληροφορίων σχετικά με τον τρόπο αντιμετώπισης των εν λόγω περιστατικών (ΙΙ).[25] Τελικό σημείο προς εξέταση, είναι η πρόταση της Ευρωπαϊκής Επιτροπής και ιδίως οι προκλήσεις, οι οποίες τίθενται αν εγκριθεί η πρόταση της (ΙΙΙ). Σε κάθε περίπτωση θα προσπαθήσουμε να δούμε την προστιθέμενη αξία και τις αδυναμίες του υπό εξέταση νομοθετικού πλαισίου και να προβούμε σε εκείνες τις αξιολογικές παρατηρήσεις που δύνανται να συμβάλλουν στη βελτίωση των τελικών ρυθμίσεων.

Ι. Οι υπάρχουσες ρυθμίσεις της Ένωσης και η επιτακτική ανάγκη θέσπισης υψηλών απαιτήσεων ασφάλειας στον κυβερνοχώρο

(Α) Η πρώτη οριζόντια νομοθεσία στο Ενωσιακό επίπεδο

Οι κυβερνοεπιθέσεις αποτελούν την τελευταία δεκαετία μια εκ των σημαντικότερων απειλών στην Ένωση.[26] Χαρακτηριστικό παράδειγμα, αποτελεί η κυβερνοεπίθεση *«WannaCry ransomware attack»* που έλαβε χώρα στις 12 Μάιου 2017, η οποία εντός λίγων ημερών κατόρθωσε να πλήξει περισσότερους από 230 χιλιάδες ηλεκτρονικούς υπολογιστές σε 150 χώρες, επηρεάζοντας κρίσιμες υποδομές, όπως το εθνικό σύστημα υγείας της Μεγάλης Βρετανίας, το σιδηροδρομικό οργανισμό *«Deutsche Bahn»* της Γερμανίας, και την κινητή τηλεφωνία *«Telefonica»* της Ισπανίας.[27]

Η ως άνω επίθεση ανέδειξε στο προσκήνιο αφενός την ανεπάρκεια αντιμετώπισης των ως άνω απειλών και την άμεση ανάγκη θέσπισης ενός

[25] Ibid 24, pp 101.

[26] Ibid *supra* 1, σελ. 192.

[27] Ibid *supra* 1, σελ. 192.

ρυθμιστικού πλαισίου. Επιπλέον, μέσω αυτής της επίθεσης διαφάνηκε πόσο σημαντικός είναι ο κυβερνόχωρος και πως μια κυβερνοεπίθεση δύναται να επηρεάσει τόσο την κοινωνία και όσο την οικονομία. Η ασφάλεια και η αξιοπιστία των ως άνω συστημάτων είναι απαραίτητες για την λειτουργία της εσωτερικής αγοράς της Ένωσης, ιδίως για την ομαλή διασυνοριακή διακίνηση υπηρεσιών αγαθών και προσώπων.[28] Επομένως, μια τέτοιας έκτασης κυβερνοεπίθεση δύναται να κλονίσει της εύρυθμη λειτουργία οικονομικών και κοινωνικών δραστηριοτήτων.[29] Άλλωστε δεν είναι τυχαίο ότι λίγους μήνες μετά την εν λόγω επίθεση, στις 13 Σεπτεμβρίου 2017, ο Πρόεδρος της Ευρωπαϊκής Επιτροπής Jean Claude Juncker ανέφερε ότι *«οι κυβερνοεπιθέσεις μπορεί να αποτελέσουν μεγαλύτερη απειλή στην αποσταθεροποίηση δημοκρατιών και οικονομιών από ότι τα όπλα και τα τανκς […].Οι κυβερνοεπιθέσεις δεν γνωρίζουν σύνορα και κανένας δεν είναι άτρωτος απέναντί τους»*.[30]

Ωστόσο πριν από την εν λόγω επίθεση είχαν γίνει ήδη σε ευρωπαϊκό επίπεδο ορισμένες προσπάθειες αντιμετώπισης των ως άνω απειλών κατά του κυβερνοχώρου. Η πρώτη έλαβε χώρα στο πλαίσιο του Συμβουλίου της Ευρώπης το 2001 με την υπογραφή της «*Διεθνούς Σύμβασης για την καταπολέμηση των εγκλημάτων Κυβερνοχώρου*», ήτοι Cybercrime Convention γνωστή και ως «*Σύμβαση της Βουδαπέστης»*.[31] Η εν λόγω σύμβαση αφορούσε κυρίως την εναρμόνιση των ποινικών νομοθεσιών μεταξύ των συμβαλλόμενων μερών.[32] Ειδικότερα μέσω της θέσπισης

[28] Maria Theres Holzleitner, Johannes Reichl, «European provisions for cyber security in the smart grid – an overview of the NIS-directive», *Elektrotechnik Und Informationstechnik*, Vol 134, No. 1, 2017, pp. 14.

[29] Ibid 28, pp. 14-15.

[30] Ibid supra 1, σελ. 192.

[31] Ibid supra 1, σελ. 192.

[32] Ibid *supra* 1, σελ. 192.

κανόνων που αφορούν παραβιάσεις της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών δεδομένων και συστημάτων.[33]

Εν συνεχεία ακολούθησε μια δεύτερη προσπάθεια με την προσθήκη πρόσθετου Πρωτοκόλλου σχετικά με την ποινικοποίηση της διασποράς ρατσιστικών και ξενοφοβικών μηνυμάτων μέσω ηλεκτρονικών υπολογιστών.[34] Ακολούθως, στις 28 Δεκεμβρίου 2008, υιοθετήθηκε και η Ευρωπαϊκή Οδηγία 2008/114 *«σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας και την εκτίμηση της ανάγκης βελτίωσης της προστασίας τους»*.[35] Η εν λόγω οδηγία έχει στόχο τον προσδιορισμό και την προστασία των κρίσιμων υποδομών.[36] Η επόμενη νομοθετική προσπάθεια της Ένωσης ήταν η υιοθέτηση της Οδηγίας 2013/40/ΕΕ «*για τις επιθέσεις κατά των πληροφοριακών συστημάτων και την κατάργηση της Απόφασης – Πλαισίου 2005/22/ΔΕΥ του Συμβουλίου*».[37] Η οδηγία αυτή έχει ως σκοπό τον προσδιορισμό των ποινικών αδικημάτων που στοχεύουν σε επιθέσεις κατά των πληροφοριακών συστημάτων και των κρίσιμων υποδομών.[38] Ωστόσο, απουσίαζε σε ενωσιακό επίπεδο ένα ρυθμιστικό πλαίσιο που να καθορίζει κοινές απαιτήσεις διασφάλισης της ασφάλειας του κυβερνοχώρου, καθώς τα κράτη μέλη της Ένωσης εφάρμοζαν διαφορετικές υφιστάμενες πρακτικές ετοιμότητας, ως αυτό φάνηκε και από την κυβερνοεπίθεση *«WannaCry ransomware attack»*, για την αντιμετώπιση τέτοιων απειλών.

[33] Ibid *supra* 1, σελ. 192.

[34] Ibid *supra* 1, σελ. 192.

[35] Ibid *supra* 1, σελ. 192.

[36] Ibid *supra* 1, σελ. 192.

[37] Ibid *supra* 1, σελ. 192.

[38] Ibid *supra* 1, σελ. 192.

Ήδη από το 2013, δηλαδή πριν από το εν λόγω περιστατικό κυβερνοασφάλειας, η Ευρωπαϊκή Επιτροπή και ο Ύπατος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας ανακοίνωσαν ότι κατά την περίοδο 2015-2020 η ασφάλεια και η αξιοπιστία του κυβερνοχώρου αποτελεί άμεση προτεραιότητα της Ευρωπαϊκής Ένωσης.[39] Τέθηκαν ακολούθως οι κυριότεροι στόχοι για την πενταετία αυτή, οι οποίοι ήταν αφενός η επίτευξη της ανθεκτικότητας στον κυβερνοχώρο, η δραστική μείωση των απειλών και των περιστατικών διατάραξης στον κυβερνοχώρο, η ανάπτυξη πολιτικής άμυνας στον κυβερνόχωρο, η ανάπτυξη βιομηχανικών και τεχνολογικών πόρων για τη διασφάλιση της ασφάλειας στον κυβερνόχωρο και η θέσπιση διεθνούς πολιτικής στον κυβερνόχωρο για την προώθηση των θεμελιωδών αξιών της Ένωσης.[40] Η Επιτροπή αμέσως μετά την εν λόγω ανακοίνωση, υπέβαλε πρόταση στις 7 Φεβρουαρίου 2013 για θέσπιση σχετικού νομοθετικού πλαισίου.[41] Η τελική έγκριση όμως καθυστέρησε αρκετά λόγω διαπραγματεύσεων της Ευρωπαϊκής Επιτροπής με το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο.[42] Εντέλει, η πρόταση της Ευρωπαϊκής Επιτροπής οριστικοποιήθηκε τον Ιούλιο του 2016.[43] Η οριστικοποίηση όμως επήλθε σε μια περίοδο που οι απειλές στον κυβερνόχωρο ήταν συνεχείς.[44] Ειδικότερα, κατά το έτος 2016 σύμφωνα με επίσημα στοιχεία της Ευρωπαϊκής Ένωσης 4.000 κυβερνοεπιθέσεις διεξάγονταν ημερησίως, σημειώνοντας αύξηση της τάξεως 300% σε σχέση με το

[39] Ibid *supra* 18, pp. 105.

[40] Renne Wilson; Stephen J. Shine, «Is Your Data Protected? A Look at Cybersecurity Regulations in the US and EU», *International In-House Counsel Journal*, Vol 10, No. 40, 2017, pp. 8-9.

[41] Charlott Walker-Osborn, Nisha Patel, «EU Cybersecurity Directive», *Oxford University Press*, 2014, pp. 38-39.

[42] Aleksandrowicz, Tomasz «The Act on the National Cybersecurity System as an Implementation of the NIS Directive», *Internal Security*, 2020, Vol. 12 Issue 1, p180-181.

[43] Ibid 42, pp. 180-181.

[44] Ibid *supra* 42, pp. 180-181.

2015.[45] Περαιτέρω, από τα εν λόγω επίσημα στοιχεία, διαφάνηκε ότι το 87% των πολιτών της Ένωσης δήλωσε ότι οι κυβερνοεπιθέσεις αποτελούν μια σοβαρή απειλή για την Ένωση.[46] Τα ως άνω μεγάλα ποσοστά υποδείκνυαν την επιτακτική ανάγκη θέσπισης περαιτέρω ρυθμίσεων.

Αν και η τελική συμφωνία των μερών θεωρήθηκε ως το αποτέλεσμα της συναίνεσης της Ευρωπαϊκής Επιτροπής, του Ευρωπαϊκού Κοινοβουλίου και Ευρωπαϊκού Συμβουλίου, το τελικό κείμενο που υιοθετήθηκε είναι πολύ πιο λιτό σε σχέση με το αρχικό προσχέδιο που υπέβαλε η Ευρωπαϊκή Επιτροπή.[47] Οι διαφοροποιήσεις μεταξύ των θεσμικών οργάνων κατά τη νομοθετική διαδικασία αφορούσαν κυρίως το πεδίο εφαρμογής, το πεδίο εναρμόνισης και τους μηχανισμούς ασφάλειας.[48] Πράγματι συγκριτικά με την πρόταση της Επιτροπής, το πεδίο εφαρμογής όπως τελικά προσδιορίστηκε είναι αρκετά περιοριστικό, καθώς δεν εντάχθηκαν όλοι οι τομείς που είχαν αρχικά προταθεί, όπως η δημόσια διοίκηση.[49] Εντέλει, η ανωτέρω οδηγία δημοσιεύθηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης στις 6 Ιουλίου 2016 και κατά την εικοστή ημέρα από τη δημοσίευση της, τέθηκε σε ισχύ.[50] Από τις 8 Αυγούστου 2016 που ετέθη σε ισχύ τα κράτη μέλη είχαν στη διάθεσή τους 21 μήνες για να την ενσωματώσουν στην εθνική τους νομοθεσία.[51] Η προθεσμία έληξε στις 9 Μαΐου 2018 και η Οδηγία έπρεπε να καταστεί δεσμευτική

[45] Ibid supra 1, σελ. 192.

[46] Ibid supra 1, σελ. 192.

[47] Ibid supra 42, pp. 180-181.

[48] Ibid supra 42, pp. 180-181.

[49] Ibid supra 41, pp. 38

[50] Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L1148

[51] Ibid *supra* 28, pp. 14.

για όλα τα κράτη μέλη της Ένωσης.[52] Ωστόσο στην πράξη η οδηγία *«ξεκίνησε»* να εφαρμόζεται καθολικά από τις 9 Νοεμβρίου του 2018, όπως θα εξηγηθεί κατωτέρω.

Η *«Οδηγία (ΕΕ) 2016/1148 για την ασφάλεια των συστημάτων δικτύου και πληροφορίων»,* η οποία είναι ευρέως γνωστή και ως *«Οδηγία NIS»*, είναι η πρώτη οριζόντια νομοθεσία που διέπει τα ζητήματα τα οποία άπτονται της ασφάλειας του κυβερνοχώρου στην Ένωση.[53] Η θέσπιση της οδηγίας αποτελούσε επείγουσα ανάγκη για την Ένωση, ως εξηγήθηκε ανωτέρω, ιδίως για την ενίσχυση της ασφάλειας και την αντιμέτωπη των αυξανόμενων απειλών.[54] Το κατεπείγον της ρύθμισης προκύπτει και από την αιτιολογική σκέψη 2 του προοιμίου της οδηγίας, η οποία αναφέρει ότι *«το μέγεθος, η συχνότητα και ο αντίκτυπος των συμβάντων ασφάλειας αυξάνονται και συνιστούν μείζονα απειλή»* και ότι *«τέτοια συμβάντα μπορούν να παρεμποδίσουν την άσκηση οικονομικών δραστηριοτήτων, να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των χρηστών και να προκαλέσουν σημαντική ζημία στην οικονομία της Ένωσης».*[55]

Η παρούσα οδηγία ως προς το επίπεδο εναρμόνισης καθορίζει τα απαιτούμενα μέτρα που πρέπει να υιοθετηθούν από τα κράτη μέλη για την ενίσχυση με ομοιόμορφο τρόπο της ασφάλειας σε ολόκληρη την Ένωση.[56] Η ομοιομορφία στον τρόπο αντιμετώπισης των κινδύνων είναι απαραίτητη καθότι όπως αναφέρεται και στο προοίμιο της οδηγίας, τα συστήματα δικτύου και πληροφορίων διαδραματίζουν ζωτικό ρόλο στη λειτουργία της εσωτερικής αγοράς στην Ένωση.[57] Τα κράτη μέλη

[52] Ibid supra 42, pp. 180.

[53] Ibid supra 14, pp. 1-3.

[54] Bragner Calle, «Supporting cybersecurity: The NIS Directive», *agendaNi*, 2018, Issue 91, p82.

[55] Ibid *supra* 50, Αιτιολογική Σκέψη 2 της Οδηγίας.

[56] Ibid *supra* 50, Αιτιολογική Σκέψη 5 της Οδηγίας.

[57] Ibid *supra* 50, Αιτιολογική Σκέψη 1 της Οδηγίας.

της Ένωσης ωστόσο είναι διαφορετικά προετοιμασμένα για την αντιμετώπιση των απειλών, ως διαφάνηκε από τα περιστατικά που έπληξαν την εσωτερική αγορά της Ένωσης.[58] Οι υφιστάμενες διαφορετικές πρακτικές αντιμετώπισης στο επίπεδο των κρατών μελών δεν επαρκούν για την διασφάλιση της κυβερνοασφάλειας, όπως καταγράφεται και στην αιτιολογική σκέψη 5 του προοιμίου της Οδηγίας.[59] Για το λόγο αυτό και η οδηγία στοχεύει στον καθορισμό ενός ελάχιστου επιπέδου ασφάλειας μέσω κοινών απαιτήσεων ενώ ταυτόχρονα ενθαρρύνει τα κράτη μέλη να συνεργάζονται και να ενεργούν κατά τρόπο ομοιόμορφο.[60]

Για την επίτευξη της καθολικής και αποτελεσματικής συνεργασίας των κρατών μελών απαιτείται μια σφαιρική προσέγγιση προς αποφυγή του κατακερματισμού των προσεγγίσεων που θα οδηγούσε σε ανομοιομορφία ως προς το επίπεδο προστασίας στην Ένωση.[61] Η επίτευξη της ασφάλειας επιτυγχάνεται με τις *«απαιτήσεις ασφάλειας και κοινοποίησης»* που επιβάλει η οδηγία στους *«φορείς εκμετάλλευσης βασικών υπηρεσιών»* και στους *«παρόχους ψηφιακών υπηρεσιών»*.[62] Ως προς τους μηχανισμούς ασφάλειας, η οδηγία ενθαρρύνει τα κράτη μέλη να συστήσουν αρμόδια εθνικά όργανα για την αντιμέτωπη των περιστατικών και να εντείνουν τη συνεργασία μεταξύ τους μέσω της δημιουργίας μιας κουλτούρας που θα επιτρέπει τη διευκόλυνση ανταλλαγής πληροφορίων και το συντονισμό στην αντιμετώπιση των διάφορων περιστατικών.[63] Μέσω των κατευθυντήριων οδηγιών επιδιώκεται περαιτέρω η ετοιμότητα των κρατών μελών για την αντιμετώπιση των

[58] Ibid *supra* 6, pp. 432-433.

[59] Ibid *supra* 6, pp. 432-433.

[60] Ibid *supra* 6, pp. 432-433.

[61] Ibid *supra* 14, pp. 3-6.

[62] Ibid supra 28, pp. 15.

[63] Ibid *supra* 50 (Βλ. Αιτιολογικές Σκέψεις).

κινδύνων και η βελτίωση της συνεργασίας τους ώστε να επιτυγχάνεται ομοιόμορφος χειρισμών των περιστατικών.[64] Ειδικότερα, η Οδηγία θέτει πέντε κύριους στόχους για τα κράτη μέλη. Καταρχάς κάθε κράτος μέλος θα πρέπει να υιοθετήσει μια εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.[65] Ακολούθως, κάθε κράτος μέλος θα πρέπει να ορίσει τρεις νέους εθνικούς οργανισμούς: τις εθνικές αρμόδιες αρχές, τα ενιαία κέντρα επαφής και τις ομάδες απόκρισης συμβάντων.[66] Οι εν λόγω εθνικοί οργανισμοί θα συμβάλουν στην επίτευξη των εθνικών στρατηγικών για την ασφάλεια των συστημάτων δικτύου και πληροφορίων.[67] Εν συνεχεία, κάθε κράτος μέλος θα πρέπει να προσδιορίσει τους φορείς εκμετάλλευσης βασικών υπηρεσιών που βρίσκονται στην επικράτεια του, οι οποίοι θα πρέπει να συμμορφώνονται στις απαιτήσεις ασφάλειας και κοινοποίησης που καθορίζει η εν λόγω οδηγία.[68] Αντίστοιχες, απαιτήσεις ασφάλειας και κοινοποίησης έχουν και οι πάροχοι ψηφιακών υπηρεσιών που βρίσκονται στην επικράτεια κάθε κράτους μέλους της Ένωσης.[69] Επιπροσθέτως, κάθε κράτος μέλος θα πρέπει να δημιουργήσει μια Ομάδα Απόκρισης Συμβάντος για την ασφάλεια των υπολογιστών «*δίκτυο CSIRT*» για την ταχεία και αποτελεσματική συνεργασία μεταξύ των κρατών μελών.[70] Τέλος, κάθε κράτος μέλος θα πρέπει να δημιουργήσει μια ομάδα συνεργασίας αφενός για την υποστήριξη της εθνικής του στρατηγικής και αφετέρου για την διευκόλυνση της συνεργασίας του με άλλα κράτη μέλη για την ανταλλαγή πληροφορίων ώστε να επιτυγχάνεται ο καλύτερος δυνατός χειρισμός των

[64] Ibid *supra* 50 (Βλ. Αιτιολογικές Σκέψεις).

[65] Ibid *supra* 42, pp. 181.

[66] Ibid *supra* 28, pp. 15.

[67] Ibid *supra* 28, pp. 15

[68] Ibid *supra* 28, pp. 15.

[69] Ibid *supra* 28, pp. 15.

[70] Ibid *supra* 28, pp. 15.

κινδύνων που εμφανίζονται.[71] Μέσω των ομάδων απόκρισης που θα δημιουργηθούν θα αναπτυχθεί εμπιστοσύνη μεταξύ των κρατών μελών και θα εδραιωθεί η αξιοπιστία στην αντιμετώπιση των περιστατικών.[72]

Από τους ανωτέρω στόχους, φαίνεται ότι το πλαίσιο που καθορίζει η Οδηγία, που είναι ελάχιστης εναρμόνισης, δίνει στα κράτη μέλη μεγάλη διακριτική ευχέρεια και ευελιξία.[73] Αυτό έχει ως συνέπεια ότι τα κράτη μέλη μπορούν να λάβουν πιο ενισχυτικά μέτρα από τα καθοριζόμενα στην Οδηγία.[74] Πάντως το εύρος της αναγνωριζόμενης ευχέρειας δημιουργεί διάφορους προβληματισμούς ως προς την αποτελεσματικότητα των ρυθμίσεων. Ενδέχεται λόγω αυτής κάθε κράτος μέλος να ενεργήσει με τόσο διαφορετικό τρόπο ώστε να υπονομευτεί σημαντικά ο στόχος για ομοιόμορφη ρύθμιση που φαίνεται να συνδέεται με την αποτελεσματικότητα των ρυθμίσεων της οδηγίας. Θα δούμε αυτό το σημείο προβληματισμού και κατωτέρω.

(Β) Ο μη σαφής προσδιορισμός των εννοιών της «κυβερνοασφάλειας» και του «κυβερνοχώρου»

Οι ως άνω στόχοι της οδηγίας έχουν ως απώτερο στόχο τη διασφάλιση της κυβερνοασφάλειας στο επίπεδο της Ευρωπαϊκής Ένωσης. Εντούτοις, παρατηρείται ότι δε γίνεται καμία αναφορά στο κείμενο αυτής στις έννοιες της κυβερνοασφάλειας και του κυβερνοχώρου.[75] Η έννοια της κυβερνοασφάλειας είναι ευρεία και χρησιμοποιείται κυρίως για την επεξήγηση του κυβερνοχώρου και της κυβερνοεπίθεσης.[76] Το πρώτο συνθετικό της κυβερνοασφάλειας προέρχεται από την

[71] Ibid *supra* 28, pp. 15.

[72] Ibid *supra* 50 (Βλ. Αιτιολογικές Σκέψεις).

[73] Ibid *supra* 42, pp. 181.

[74] Ibid *supra* 42, pp. 181.

[75] Ibid *supra* 6, pp. 425-426.

[76] Ibid *supra* 6, pp. 426.

αγγλική λέξη *«cyber»* η οποία αφορά την *«σύνδεση στο διαδίκτυο»*.[77] Η συνεχής εξέλιξη της τεχνολογίας και κατ' επέκταση των δυνατοτήτων του διαδικτύου κάνει πιο δύσκολο το έργο των επιστημόνων και του νομοθέτη που προσπαθούν για έναν ακριβή προσδιορισμό της ως άνω έννοιας. Ο μη σαφής προσδιορισμός της διαφαίνεται και από τις διαφορετικές ερμηνείες που υιοθετούνται από διάφορες μελέτες και νομικά κείμενα.[78] Σε μια προσπάθεια προσδιορισμού της έννοιας η διεθνής ομάδα εμπειρογνωμόνων που συνέταξε το εγχειρίδιο *«Tallin Manual of the International Law Applicable to Cyber Warfare»* όρισαν την κυβερνοασφάλεια ως *«την επιχείρηση στον κυβερνοχώρο, είτε επιθετική είτε αμυντική, που αναμένεται να προκαλέσει τραυματισμό ή θάνατο σε ανθρώπους ή σημαντική υλική ζημία και καταστροφή σε αντικείμενα» και* την επιχείρηση στον κυβερνοχώρο και «*την εφαρμογή συγκεκριμένων δυνατοτήτων, μέσω του κυβερνοχώρου, με πρωταρχικό σκοπό την επίτευξή συγκριτικού πλεονεκτήματος είτε εντός του κυβερνοχώρου είτε στα συμβατικά πεδία επιχειρήσεων μέσω του κυβερνοχώρου*».[79] Παράλληλα, στον Αμερικάνικο Νόμο *«Internet of Things Cybersecurity Improvement (IoT Cybersecurity Act)»* η έννοια της κυβερνοασφάλειας συσχετίζεται με τις «*έξυπνες συσκευές»* και τα ζητήματα της σύνδεσης στο διαδίκτυο.[80] Από τους δύο ανωτέρω ορισμούς διαφαίνεται ότι δεν υπάρχει επαρκής ευθυγράμμιση ως προς τον προσδιορισμό της έννοιας της κυβερνοασφάλειας.[81] Πάρα ταύτα, αυτό που γίνεται αντιληπτό από τα ανωτέρω κείμενα είναι ότι ο απώτερος σκοπός της

[77] Grazyna Szpor, «The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland», *Review of European and Comparative Law*, Vol 46, Issue 3, 2021, pp. 223

[78] Ibid *supra* 6, pp. 425.

[79] Ibid *supra* 1, σελ. 192.

[80] Ibid *supra* 6, pp. 435-438.

[81] Ibid *supra* 6, pp. 435-438.

κυβερνοασφάλειας είναι η προστασία του κυβερνοχώρου.[82] Η έννοια του κυβερνοχώρου αν και δεν είναι σαφής θα μπορούσε να οριστεί ως «το παγκόσμιο πληροφοριακό περιβάλλον, το οποίο δημιουργείται από τη διασύνδεση αυτοματοποιημένων πληροφοριακών συστημάτων».[83] Πρόκειται στην πραγματικότητα για έναν εικονικό και διαδραστικό χώρο.[84]

Οι απροσδιόριστες ανωτέρω έννοιες αποτέλεσαν και ένα εκ των λόγων των έντονων διαβουλεύσεων της Επιτροπής με το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο.[85] Στην αρχική πρόταση της η Επιτροπή συμπεριλαμβάνει την έννοια *«ασφάλεια»* ωστόσο στο τελικό κείμενο της οδηγίας εντάχθηκε η έννοια της *«ασφάλειας των συστημάτων δικτύου και πληροφοριών».*[86] Από το κείμενο προκύπτει ότι η έννοια του κυβερνοχώρου δεν καταγράφεται στο κείμενο της οδηγίας ωστόσο υποδηλώνεται από την έννοια *«των συστημάτων δικτύου και πληροφοριών»*.[87] Ειδικότερα, σύμφωνα με το άρθρο 4 της Οδηγίας ως σύστημα δικτύου και πληροφορίων ορίζεται *«κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων ή ψηφιακών δεδομένων που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους».*[88] Εντός της ανωτέρω έννοιας

[82] Ibid *supra* 6, pp. 425.

[83] Ibid *supra* 1, σελ, 192.

[84] Ibid *supra* 1, σελ, 192.

[85] Ibid *supra* 77, pp. 223.

[86] Πρόταση Ευρωπαϊκής Επιτροπής «Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση», ημερομηνίας 2/2/2013. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A52013PC0048

[87] Ibid *supra* 6, pp. 433-436.

[88] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

συμπεριλαμβάνεται συνεπώς και *το «δίκτυο ηλεκτρονικών επικοινωνιών κατά την έννοια του άρθρου 2 στοιχείο α) της οδηγίας 2002/21/ΕΚ».*[89]

Η ασφάλεια των συστημάτων δικτύου και πληροφοριών ορίζεται από την Οδηγία NIS ως *«η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, σε δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών».*[90] Η ασφάλεια των συστημάτων δικτύου και πληροφορίων συνιστά επιτακτική ανάγκη, καθώς ως αναφέρει η αιτιολογική σκέψη 3 της ανωτέρω οδηγίας τυχόν διακοπή των υπηρεσιών τους, είτε εσκεμμένη είτε μη, ανεξάρτητα από τον τόπο που εκδηλώνεται, επηρεάζει την Ένωση στο σύνολο της.[91] Η διακοπή των υπηρεσιών εν λόγω συστημάτων μπορεί να επέλθει από ένα συμβάν, το οποίο καθορίζεται στην εν λόγω οδηγία ως «*κάθε γεγονός που έχει στη πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών*».[92]

Συνεπώς, πρωταρχικός στόχος της παρούσας Οδηγίας είναι η διαφύλαξη των ως άνω συστημάτων από τέτοια συμβάντα. Γι' αυτό και καθορίζονται συγκεκριμένες απαιτήσεις για τον χειρισμό τους. Ο χειρισμός τέτοιων συμβάντων ορίζεται ως «*το σύνολο των διαδικασιών που υποστηρίζουν τον εντοπισμό, την ανάλυση, και την ανάσχεση ενός συμβάντος και την παρέμβαση για την αντιμετώπιση του».*[93] Εντούτοις, η αιτιολογική σκέψη 7 της Οδηγίας, αναφέρει ότι απαιτείται και η κάλυψη

[89] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[90] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[91] Ibid *supra* 50, Αιτιολογική Σκέψη 3 της Οδηγίας.

[92] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[93] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

ενδεχόμενων κινδύνων.[94] Στην αιτιολογική σκέψη 13, η οδηγία στοχεύει σε μια προληπτική αντιμετώπιση, η οποία προφανώς καλύπτει τόσο τυχόν συμβάντα όσο και ενδεχόμενους κινδύνους.[95] Ως εκ τούτου, στο άρθρο 4 της Οδηγίας, ο κίνδυνος ορίζεται ως «*κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός με δυνητική δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών*».[96]

Από τους ανωτέρω ορισμούς που παρέχονται στην υπό εξέταση οδηγία για την κατανόηση της κυβερνοασφάλειας και του κυβερνοχώρου φαίνεται ότι διαφέρει σημαντικά από αυτούς που παρέχονται από την διεθνή ομάδα εμπειρογνωμόνων και το εγχειρίδιο *«Tallin Manual of the International Law Applicable to Cyber Warfare»*, καθώς και από τον *IoT Cybersecurity Act.*[97] Από τον ως άνω ορισμό της κυβερνοασφάλειας που υιοθετείται από την διεθνή ομάδα εμπειρογνωμόνων προκύπτει ότι εντάσσει στο ορισμό της κυβερνοασφάλειας και την απειλή κατά φυσικών προσώπων με την πρόκληση τραυματισμού ή θανάτου ή οποιαδήποτε υλικής ζημίας.[98] Ενώ στην οδηγία NIS δεν γίνεται καμία αναφορά στο ενδεχόμενο επηρεασμού των φυσικών προσώπων μέσα από την αναφορά στην ασφάλεια των συστημάτων δικτύου και πληροφορικής. Επιπλέον, ο Αμερικάνικος Νόμος, ήτοι *IoT Cybersecurity Act* παρέχει ένα ευρύτερο ορισμό από αυτόν που δίδει η οδηγία NIS.[99] Η Οδηγία NIS, ως θα επεξηγηθεί κατωτέρω, ρυθμίζει ένα πολύ περιοριστικό υποκειμενικό πεδίο εφαρμογής.[100]

[94] Ibid *supra* 50, Αιτιολογική Σκέψη 7 της Οδηγίας.

[95] Ibid *supra* 50, Αιτιολογική Σκέψη 7 της Οδηγίας.

[96] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[97] Ibid *supra* 6, pp. 425.

[98] Ibid *supra* 1, σελ. 192.

[99] Ibid *supra* 6, pp. 437.

[100] Ibid *supra* 6, pp. 437.

(Γ) Το στενό υποκειμενικό πεδίο εφαρμογής της Οδηγίας NIS

Ως προς το υποκειμενικό πεδίο εφαρμογής της Οδηγίας, δύο είναι οι κατηγορίες των οντοτήτων που καλύπτονται από την παρούσα οδηγία.[101] Η πρώτη κατηγορία αφορά τους *«φορείς εκμετάλλευσης βασικών υπηρεσιών»* και η δεύτερη τους *«παρόχους ψηφιακών υπηρεσιών»*.[102] Σύμφωνα με το άρθρο 4 της οδηγίας ως φορείς εκμετάλλευσης βασικών υπηρεσιών θεωρούνται οι *«δημόσιες ή ιδιωτικές οντότητες»* οι οποίες εντάσσονται στους τομείς του Παραρτήματος ΙΙ και οι οποίες «*πληρούν τα κριτήρια που ορίζονται στο άρθρο 5, παράγραφος 2»* της Οδηγίας.[103]

Οι τομείς που εντάσσονται στο Παράρτημα ΙΙ είναι επτά.[104] Είναι ειδικότερα η ενέργεια, οι μεταφορές, οι τράπεζες, οι υποδομές χρηματοπιστωτικών αγορών, ο τομέας της υγείας, η προμήθεια και διανομή πόσιμου νερού, καθώς και η ψηφιακή υποδομή.[105] Στο Παράρτημα ΙΙ καθορίζονται επίσης και οι υποτομείς κάθε τομέα και ειδικότερα το είδος της οντότητας του κάθε υποτομέα.[106] Από τον κατάλογο του Παραρτήματος ΙΙ είναι αντιληπτό ότι οι τομείς και υποτομείς που εντάσσονται στο πεδίο εφαρμογής της παρούσας οδηγίας είναι συγκεκριμένοι.[107] Ωστόσο ο εν λόγω κατάλογος δεν είναι εξαντλητικός. Για παράδειγμα, η Αυστρία, η Κροατία, η Κύπρος, η Λιθουανία, η Μάλτα, η Σλοβακία, η Ισπανία και η Ελβετία έχουν εντάξει και τη

[101] Sandra Cassotta, Maria Pettersson, «Climate change, environmental threats and cyber-threats to critical infrastructures in multi-regulatory sustainable global approach with Sweden as an example», *Beijing Law Review*, 2019, Vol. 10, No. 3, pp. 635-636.

[102] Ibid 101, pp. 635-636.

[103] Ibid *supra* 14, pp. 3-6.

[104] Ibid *supra* 14, pp. 3-6

[105] Ibid *supra* 50, Παράρτημα ΙΙ της Οδηγίας.

[106] Ibid *supra* 50, Παράρτημα ΙΙ της Οδηγίας.

[107] Ibid *supra* 14, pp. 3-6.

δημόσια διοίκηση.[108] Επιπλέον, η Γαλλία είναι η μόνη που έχει προσθέσει και την εκπαίδευση ενώ η Ισπανία είναι η μόνη χώρα που έχει εντάξει τα διαστημικά και ερευνητικά κέντρα.[109] Βλέπουμε λοιπόν πως η ευχέρεια οδηγεί σε ανομοιομορφία. Γι' αυτό και ορισμένοι σχολιαστές έχουν αναφέρει ότι υπάρχουν τομείς που δεν έχουν συμπεριληφθεί στο Παράρτημα ΙΙ και οι οποίοι θα πρέπει μελλοντικά να ενταχθούν, όπως η δημόσια διοίκηση, ο ταχυδρομικός τομέας, ο τομέας τροφίμων, η χημική και πυρηνική βιομηχανία, ο περιβαλλοντικός τομέας και η πολιτική προστασία.[110]

Περαιτέρω, σύμφωνα με την παράγραφο 2 του άρθρου 5 της ανωτέρω οδηγίας, τα κριτήρια που θα πρέπει να κατέχει μια οντότητα, είτε ιδιωτική είτε δημόσια, για να θεωρείται ότι εντάσσεται σε οποιοδήποτε τομέα του Παραρτήματος ΙΙ είναι τα ακόλουθα: *«(α)να παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών και ή οικονομικών δραστηριοτήτων», « (β) η παροχή της υπηρεσίας αυτής να στηρίζεται σε συστήματα δικτύου και πληροφορίων»* και *«(γ) τυχόν συμβάν στη λειτουργία του συστήματος δικτύου και πληροφοριών»* να μπορεί να «*προκαλέσει σοβαρή διατάραξη της παροχής της εν λόγω υπηρεσίας».*[111]

Ως προς το σημείο (α), η έννοια της «*ουσιώδης παροχής*» δεν επεξηγείται επαρκώς στην εν λόγω οδηγία. Αυτό έχει ως συνέπεια να παρέχεται η δυνατότητα στα κράτη μέλη να αποφασίσουν ποιους φορείς θεωρούν ότι παρέχουν «ουσιώδη» υπηρεσία στην επικράτεια τους.[112] Ως ουσιώδης παροχή ενδέχεται να θεωρηθεί αυτή

---

[108] Nicolas Van Tieghem, Nicolas Lefebvre, «While preparing the NIS 2, update of the European overview of NIS transposition by the Member States…toward convergence ?», RiskInsight , Πρόσβαση 1/11/2021. https://www.riskinsight-wavestone.com/en/2021/09/en-pleine-preparation-de-la-nis-v2-mise-a-jour-du-tour-dhorizon-europeen-de-transposition-de-la-directive-nis-par-les-etats-membres-vers-une-convergence/

[109] Ibid 108.

[110] Ibid *supra* 14, pp. 3-6.

[111] Ibid *supra* 50, Άρθρο 5 της Οδηγίας.

[112] Ibid *supra* 20, pp. 54-56.

που σε περίπτωση διατάραξης, είναι πιθανό να προκαλέσει σοβαρές και δυσμενές επιπτώσεις σε οικονομικές και κοινωνικές δραστηριότητες.[113] Παράδειγμα τέτοιων επιπτώσεων μπορεί να έχουμε όταν από ένα περιστατικό μπορεί να επηρεαστούν και άλλες υφιστάμενες οντότητες στην επικράτεια ενός κράτους μέλους παραλύοντας κατ' αυτόν τον τρόπο την οικονομία.[114] Συνεπώς, ο ρόλος του κάθε φορέα εκμετάλλευσης βασικών υπηρεσιών και η κρισιμότητά του για κάθε κράτος μέλος θα πρέπει να αξιολογηθεί από το ίδιο το κράτος.[115] Η αξιολόγηση αυτή είναι εγγενώς υποκειμενική.[116] Θα ήταν προτιμότερο η ίδια η οδηγία να καθόριζε ένα ή και περισσότερα αντικειμενικά κριτήρια αξιολόγησης της ένταξης των φορέων εκμετάλλευσης βασικών υπηρεσιών.

Ως προς το σημείο (γ) που αφορά τον προσδιορισμό της σοβαρότητας μιας διατάραξης θα πρέπει να λαμβάνονται κατά το άρθρο 6 της οδηγίας τα ακόλουθα στοιχεία: «*ο αριθμός των χρηστών που εξαρτώνται από την υπηρεσία που παρέχεται από την οικεία οντότητα, η εξάρτηση άλλων τομέων που αναφέρονται στο παράρτημα ΙΙ από την υπηρεσία που παρέχεται από την εν λόγω οντότητα, ο αντίκτυπος που θα μπορούσαν να έχουν τα συμβάντα, από άποψη βαθμού και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες ή στη δημόσια ασφάλεια, το μερίδιο αγοράς της εν λόγω οντότητας, το γεωγραφικό εύρος της περιοχής που θα μπορούσε να επηρεαστεί από ένα συμβάν και η σημασία του φορέα για τη διατήρηση επαρκούς επιπέδου της υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω υπηρεσίας*».[117] Τα τρία αυτά κριτήρια θα πρέπει να ισχύουν σωρευτικά για να

[113] Ibid *supra* 20, pp. 54-56.

[114] Ibid *supra* 20, pp. 54-56.

[115] Ibid *supra* 20, pp. 54-56.

[116] Ibid *supra* 20, pp. 54-56.

[117] Ibid supra 50, Άρθρο 6 της Οδηγίας.

χαρακτηριστεί η εν λόγω οντότητα ως φορέας εκμετάλλευσης βασικών υπηρεσιών.[118] Επομένως, τα κράτη μέλη όταν διαπιστώσουν ότι μια οντότητα εντάσσεται στο Παράρτημα ΙΙ της οδηγίας, οφείλει εν συνεχεία να εξετάσει εάν πληροί τα τρία αυτά κριτήρια για να εντάσσεται το πεδίο εφαρμογής της οδηγίας.

Εκ των ανωτέρω, ανακύπτει σαφώς πως δεν εμπίπτουν όλοι οι φορείς εκμετάλλευσης βασικών υπηρεσιών του Παραρτήματος ΙΙ στο πεδίο εφαρμογής της Οδηγίας.[119] Η οδηγία ναι μεν παρέχει ορισμένα κριτήρια για τον προσδιορισμό ενός φορέα εκμετάλλευση βασικών υπηρεσιών, ωστόσο εναπόκειται στο κάθε κράτος μέλος να καθορίσει ποιους κρίνει τελικά ως φορείς εκμετάλλευσης βασικών υπηρεσιών και ως ερμηνεύει το ίδιο την έννοια «ουσιώδη παροχή».

Περαιτέρω, το άρθρο 5, παράγραφος 1 της οδηγίας έδωσε στα κράτη μέλη, τη δυνατότητα έως τις 9 Μαΐου 2018 να έχουν ενσωματώσει την οδηγία, και επιπλέον χρονικό περιθώριο έξι μηνών, δηλαδή έως τις 9 Νοεμβρίου το 2018, για να προσδιορίσουν για κάθε τομέα και υποτομέα τους φορείς εκμετάλλευσης βασικών υπηρεσιών που βρίσκονται στην επικράτεια τους, υπό το φως των ανωτέρων κριτηρίων.[120] Η διάταξη αυτή επί της ουσίας δίνει στα κράτη μέλη τη δυνατότητα διαφοροποίησης ως προς την πραγματική «έναρξη» των υποχρεώσεων των φορέων εκμετάλλευσης βασικών υπηρεσιών έως και ένα εξάμηνο μετά το πρώτο εξάμηνο έναρξης της εφαρμογής της Οδηγίας. Αυτό έχει σαν αποτέλεσμα να παραμένουν οι υποχρεώσεις σε «*αδράνεια*» μέχρι τα κράτη μέλη να προσδιορίσουν τους φορείς εκμετάλλευσης βασικών υπηρεσιών. Συνεπώς, οι υποχρεώσεις απορρέουν για τους παρόχους ψηφιακών υπηρεσιών από τις 9 Μαΐου ενώ για τους φορείς εκμετάλλευσης

[118] Ibid *supra* 14, pp. 3-6.

[119] Ibid *supra* 14, pp. 3-6.

[120] Ibid *supra* 50, Άρθρο 5 της Οδηγίας.

βασικών υπηρεσιών όταν και όποτε προσδιοριστούν από τα κράτη και πάντως εντός του πρώτου εξαμήνου από την έναρξη της άμεσης ισχύος της Οδηγίας. Από έχει ως αποτέλεσμα να μην τυγχάνει καθολικής εφαρμογής η Οδηγία εξ υπαρχής και για τις δυο κατηγορίες οντοτήτων.

Επιπροσθέτως, ο κατάλογος των αναγνωρισμένων φορέων εκμετάλλευσης βασικών υπηρεσιών που υποβλήθηκε ήδη από κάθε κράτος μέλος, θα πρέπει κάθε δύο χρόνια να ανανεώνεται για να εντάσσονται νέες οντότητες και για να επανεξετάζεται εάν οι υφιστάμενες οντότητες συνεχίζουν να πληρούν τα κριτήρια που θέτει η οδηγία.[121] Ωστόσο, το ερώτημα που ανακύπτει είναι τι θα συμβεί σε περίπτωση που παραλειφθεί να συμπεριληφθεί ένας φορέας εκμετάλλευσης βασικών υπηρεσιών εντός της αρχικώς ορισθείσας προθεσμίας. Θα πρέπει να περιμένει ένα κράτος μέλος δυο έτη για να την συμπεριλάβει μεταγενέστερα στον αναθεωρημένο κατάλογο; Σύμφωνα με τους σχολιαστές, ενδεχομένως ορισμένα κράτη μέλη να συμπεριέλαβαν ένα εκτενή κατάλογο φορέων προληπτικά με κύριο σκοπό να αποφύγουν ενδεχόμενες κυρώσεις από ελλείψεις που ήταν πιθανές λόγω της ασάφειας των κριτηρίων που χρησιμοποιεί το άρθρο 5 παράγραφος 2.[122]

Η δεύτερη κατηγορία που εντάσσεται στο πεδίο εφαρμογής της παρούσας οδηγίας είναι οι πάροχοι ψηφιακών υπηρεσιών.[123] Πάροχοι ψηφιακών υπηρεσιών θεωρούνται σύμφωνα με το άρθρο 4 τα *«νομικά πρόσωπα που παρέχουν ψηφιακές υπηρεσίες».*[124] Οι ψηφιακές υπηρεσίες ορίζονται ως *«οι υπηρεσίες κατά την έννοια του άρθρου 1 παράγραφος 1 της οδηγίας (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου*

[121] Ibid *supra* 14, pp. 3-6.

[122] Ibid *supra* 14, pp. 3-6.

[123] Ibid *supra* 14, pp. 3-6.

[124] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

και του Συμβουλίου (1) οι οποίες αναφέρονται στο παράρτημα ΙΙΙ».[125] Σύμφωνα με το Παράρτημα ΙΙΙ της οδηγίας τα είδη των ψηφιακών υπηρεσιών που εντάσσονται στο πεδίο εφαρμογής της παρούσας οδηγίας είναι οι επιγραμμικές αγορές, οι επιγραμμικές μηχανές αναζήτησης και οι υπηρεσίες νεφοϋπολογιστικής.[126] Οι παρόχοι ψηφιακών υπηρεσιών λόγω του διασυνοριακού τους χαρακτήρα, δεν προσδιορίζονται από τα κράτη μέλη, άλλα από την ίδια την οδηγία.[127] Συνεπώς, εντάσσονται όλοι αυτόματα.

Ως επιγραμμική αγορά ορίζεται η «*ψηφιακή υπηρεσία που επιτρέπει σε καταναλωτές και/ή εμπόρους […]να συνάπτουν επιγραμμικές συμβάσεις πώλησης ή παροχής υπηρεσιών με εμπόρους είτε στον ιστοχώρο της επιγραμμικής αγοράς είτε σε ιστοχώρο εμπόρου που χρησιμοποιεί υπηρεσίες υπολογιστικής παρεχόμενες από την επιγραμμική αγορά».*[128] Παραδείγματα επιγραμμικών αγορών είναι οι ηλεκτρονικές αγορές μέσω ιστοσελίδων, όπως ASOS ή και η αγορά ηλεκτρονικών υπηρεσιών όπως αυτές που παρέχει το Netflix στους συνδρομητές του. Ως επιγραμμική μηχανή αναζήτησης ορίζεται η *«ψηφιακή υπηρεσία που επιτρέπει στους χρήστες να εκτελούν αναζητήσεις κατ' αρχήν σε όλους τους ιστοχώρους ή σε ιστοχώρους συγκεκριμένης γλώσσας βάσει ερωτήματος για οποιοδήποτε θέμα, με τη μορφή λέξης-κλειδιού, φράσης ή άλλων δεδομένων, και επιστρέφει ως αποτέλεσμα συνδέσμους όπου μπορεί κανείς να βρει πληροφορίες σχετικές με το περιεχόμενο που έχει ζητηθεί».*[129] Παραδείγματα επιγραμμικών μηχανών αναζήτησης αποτελούν η Google και η Amazon στους χρήστες. Τέλος, ως υπηρεσία νεφοϋπολογιστική ορίζεται *«η ψηφιακή υπηρεσία που*

[125] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[126] Ibid *supra* 14, pp. 3-6.

[127] Ibid *supra* 101, pp. 635-636.

[128] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[129] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

επιτρέπει την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων».[130] Τέτοιο παράδειγμα αποτελεί η δυνατότητα αγοράς από την Apple πρόσθετου χώρου αποθήκευσης στο iCloud στα iPhones.

Σύμφωνα με την αιτιολογική σκέψη 53 *«σε περίπτωση παρόχων ψηφιακών υπηρεσιών, οι απαιτήσεις αυτές δεν θα πρέπει να εφαρμόζονται στις πολύ μικρές και τις μικρές επιχειρήσεις».*[131] Συνεπώς, από το πεδίο εφαρμογής της παρούσας οδηγίας εξαιρούνται οι πολύ μικρές και μικρές οντότητες.[132] Σύμφωνα με το άρθρο 2 παράγραφος 2 της σύστασης 2003/361/ΕΚ της Επιτροπής, ως μικρή επιχείρηση θεωρείται «*η επιχείρηση που απασχολεί λιγότερους από 50 εργαζομένους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 10 εκατομμύρια ευρώ»* και ως πολύ μικρή αυτή *«η οποία απασχολεί λιγότερους από δέκα εργαζομένους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 2 εκατομμύρια ευρώ».*[133] Οι εν λόγω οντότητες εξαιρούνται καθώς τα απαιτούμενα μέτρα ασφάλειας ενδέχεται να αποτελέσουν δυσανάλογο οικονομικό βάρος για αυτές.[134] Ωστόσο, η απουσία κοινών απαιτήσεων ασφάλειας και στις μικρές οντότητες, ενδέχεται να προκαλέσει μελλοντικά προβλήματα.[135]

---

[130] Ibid *supra* 50, Άρθρο 4 της Οδηγίας.

[131] Ibid *supra* 50, Αιτιολογική Σκέψη 53 της Οδηγίας.

[132] Najmudin Saqib, Vasileios Germanos, Zeng Wen, Leandros Maglaras, «Mapping of the Security Requirements of GDPR and NIS», *EAI Endorsed Transactions on Security* & Safety , 2020, Vol. 7, Issue 24, pp 7.

[133] Σύσταση Ευρωπαϊκής Επιτροπής «Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων», ημερομηνιας 6/5/2003.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32003H0361

[134] Ibid *supra* 28, pp. 15.

[135] Ibid *supra* 28, pp. 15.

(Δ) Οι προβλεπόμενες από την Οδηγία NIS υποχρεώσεις ασφάλειας και κοινοποίησης περιστατικών

Οι δύο κατηγορίες οντοτήτων που εντάσσονται στο πεδίο εφαρμογής της οδηγίας υπόκεινται σε υποχρεώσεις ασφάλειας και κοινοποίησης περιστατικών. Οι υποχρεώσεις αυτές διαφέρουν μεταξύ των δύο κατηγοριών.[136] Ειδικότερα, σύμφωνα με την παράγραφο 1 του άρθρου 14, οι φορείς εκμεταλλεύσεις βασικών υπηρεσιών θα πρέπει λάβουν *«κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες»* με σκοπό τη διαχείριση των κινδύνων.[137] Επιπροσθέτως, στην παράγραφο 2 του ανωτέρω άρθρου καταγράφεται ότι οι φορείς εκμεταλλεύσεις θα *λαμβάνουν «κατάλληλα μέτρα για αποτροπή και ελαχιστοποίηση του αντίκτυπου των συμβάντων, για τη διασφάλιση της συνέχειας του».*[138] Από τις ανωτέρω παραγράφους ανακύπτει ότι οι απαιτήσεις ασφάλειας των φορέων εκμετάλλευσης βασικών υπηρεσιών είναι πρώτον να διαχειρίζονται τους κινδύνους και δεύτερον να διασφαλίζουν ότι θα συνεχιστεί η λειτουργία των υπηρεσιών που παρέχουν μέσω της αποτροπής και ελαχιστοποίησης των συνεπειών.[139] Προφανώς, ο κύριος σκοπός των απαιτήσεων αυτών είναι η μη διακοπή της υπηρεσιών των εν λόγω συστημάτων, καθώς εάν διακοπούν τότε ανεξάρτητα από τον τόπο εκδηλώσεως της μια τέτοια διακοπή δύναται να επηρεάσει και την λειτουργία της εσωτερικής αγοράς της Ένωσης.[140]

[136] Ibid *supra* 14, pp. 3-6.

[137] Ibid *supra* 50, Άρθρο 14 της Οδηγίας.

[138] Ibid *supra* 50, Άρθρο 14 της Οδηγίας

[139] Ibid *supra* 14, pp. 3-6.

[140] Ibid *supra* 14, pp. 3-6.

Ωστόσο, αυτό που παρατηρείται είναι ότι οι έννοιες *«κατάλληλα»* και *«αναλογικά»* δεν ερμηνεύονται από την οδηγία.[141] Αυτό, παρέχει τη δυνατότητα σε κάθε κράτος μέλος να ερμηνεύσει το ίδιο τι συνιστά αναλογικό και κατάλληλο μέτρο κατά τη δεδομένη στιγμή.[142] Προφανώς τα *«κατάλληλα και αναλογικά»* μέτρα θα πρέπει να ληφθούν από τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών με βάση την κρίση τους η οποία δε μπορεί παρά να είναι σε ένα βαθμό υποκειμενική.[143] Η αναφορά σε αναλογικά μέτρα υποδηλώνει ότι το κόστος των τεχνικών και μέτρων που θα ληφθούν θα πρέπει να είναι ανάλογα των ενδεχόμενων κινδύνων.[144] Κατ' αυτόν τον τρόπο η οδηγία προσπαθεί να αποφύγει την επιβολή δυσανάλογων οικονομικών ή και διοικητικών βαρών στις οντότητες.[145] Συνεπώς θα πρέπει να εξετάζεται κάθε φορά ο κίνδυνος και το κόστος με το επιθυμητό αποτέλεσμα της οδηγίας.[146]

Ωστόσο το ερώτημα που δημιουργείται είναι πως διασφαλίζεται ότι τα μέτρα που ελήφθησαν ήταν πράγματι κατάλληλα και αναλογικά σε κάθε συγκεκριμένη περίπτωση.[147] Το επόμενο ερώτημα που γεννιέται εν προκειμένω είναι εάν πράγματι θα καταστεί εφικτό να επιτευχθεί μια κοινή προσέγγιση και αντιμετώπιση των κινδύνων από όλα τα κράτη μέλη.[148] Όπως αναφέρθηκε και προηγουμένως, σκοπός της οδηγίας είναι η ομοιόμορφη αντιμετώπιση των κινδύνων και συμβάντων

[141] Ibid *supra* 14, pp. 3-6.

[142] Ibid *supra* 14, pp. 3-6.

[143] Johan David Michels, Ian Walden, «Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?», *European Law Review*, 2020, Vol. 45, Issue 1, p. 25.

[144] Ibid 143, pp. 35-36.

[145] Ibid *supra* 143, pp. 35-36.

[146] Ibid *supra* 143, pp. 35-36.

[147] Ibid *supra* 14, pp. 3-6.

[148] Ibid *supra* 14, pp. 3-6.

κυβερνοεπίθεσης στην Ένωση, καθώς όπως έχει παρατηρηθεί οι πρακτικές που εφάρμοζαν προηγουμένως τα κράτη μέλη δεν ήταν αρκετά για την διασφάλιση της ασφάλειας του κυβερνοχώρου.[149]

Για αυτόν ακριβώς το λόγο είναι σημαντικός ο όσο το δυνατόν πιο ακριβής καθορισμός των εννοιών. Ελλείψει ακρίβειας κατά τον προσδιορισμό των εννοιών που είναι αναγκαίες για την εφαρμογή του νομοθετικού πλαισίου είναι πιθανό να εμφανιστούν αποκλίνουσες πρακτικές από τα κράτη μέλη.[150] Επί του παρόντος, η Ευρωπαϊκή Επιτροπή ενθαρρύνει τις υπό κρίση οντότητες να εφαρμόσουν τις γενικές αρχές που εξέδωσε η Ομάδα Συνεργασίας, στις οποίες αναφέρεται ότι τα μέτρα θα πρέπει να είναι *«αποτελεσματικά, προσαρμοσμένα, συμβατά, αναλογικά, συγκεκριμένα, επαληθεύσιμά και χωρίς αποκλεισμούς».*[151] Σε κάθε περίπτωση οι κατευθυντήριες γραμμές θα συμβάλλουν στην συνεκτίμηση των ανωτέρων αρχών πριν τη λήψη μέτρων ασφάλειας.[152] Ενδεχομένως, να ήταν προτιμότερο, στο κείμενο της οδηγίας να διασφαλίζονται ορισμένες ελάχιστες απαιτήσεις.[153]

Πέραν όμως από τις απαιτήσεις ασφάλειας, το άρθρο 14 επιβάλλει και απαιτήσεις κοινοποίησης. Ειδικότερα, σύμφωνα με την παράγραφο 3 του άρθρου 14 οι φορείς εκμετάλλευσης βασικών υπηρεσιών θα πρέπει να *«κοινοποιούν χωρίς αδικαιολόγητη καθυστέρηση στην αρμόδια αρχή ή στην CSIRT συμβάντα με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών που παρέχουν. Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσει τυχόν διασυνοριακό αντίκτυπο του συμβάντος. Η κοινοποίηση δεν*

[149] Ibid *supra* 14, pp. 3-6.

[150] Ibid *supra* 14, pp. 3-6.

[151] Ibid *supra* 14, pp. 3-6.

[152] Ibid *supra* 14, pp. 3-6.

[153] Ibid *supra* 14, pp. 3-6.

συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα».[154] Από την ανωτέρω, παράγραφο ο χαρακτηρισμός «*σοβαρό»* προσδιορίζει ότι η απαίτηση της κοινοποίησης δεν απαιτείται σε κάθε συμβάν άλλα σε αυτό που κρίνεται σοβαρό από τους ίδιους τους φορείς εκμετάλλευσης βασικών υπηρεσιών.[155]

Στο άρθρο 14 παράγραφος 4 της ως άνω οδηγίας, αναφέρονται συγκεκριμένες παράμετροι που θα πρέπει να ληφθούν υπόψη κάθε φορά κατά τον προσδιορισμό της σοβαρότητας ή όχι του αντίκτυπου ενός συμβάντος.[156] Οι παράμετροι αυτές είναι *«ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας, η διάρκεια του συμβάντος και το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν».*[157] Συνεπώς, τα ανωτέρω στοιχεία θα πρέπει να συνεκτιμώνται κάθε φορά σωρευτικά για τη διαπίστωση του κατά πόσο η διατάραξη είναι όντως σοβαρή ή όχι.[158] Μέχρι σήμερα τα κριτήρια αυτά δεν έχουν εξεταστεί από το ΔΕΕ για να διαπιστωθεί το πώς ερμηνεύεται ο *«αριθμός χρηστών»*, η *«διάρκεια συμβάντος»* και το *«γεωγραφικό εύρος».*

Αντίστοιχα, οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει λάβουν *«κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες»* με σκοπό τη διαχείριση των κινδύνων.[159] Προτού λάβουν τα μέτρα που καθορίζονται οι πάροχοι βασικών υπηρεσιών θα πρέπει να συνεκτιμήσουν τα ακόλουθα στοιχεία *«α) την ασφάλεια των συστημάτων και των εγκαταστάσεων· β) τη διαχείριση συμβάντων· γ) τη διαχείριση της επιχειρησιακής συνέχειας· δ) την*

[154] Ibid *supra* 50, Άρθρο 14 της Οδηγίας.

[155] Ibid *supra* 14, pp. 3-6.

[156] Ibid *supra* 14, pp. 3-6.

[157] Ibid *supra* 50, Άρθρο 14 της Οδηγίας.

[158] Ibid *supra* 14, pp. 3-6.

[159] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

παρακολούθηση, τις επιθεωρήσεις και τις δοκιμές· ε) τη συμμόρφωση με διεθνή πρότυπα».[160] Τα προαναφερθέντα κριτήρια θα πρέπει να ληφθούν υπόψη σωρευτικά.[161] Δεν είναι τυχαία η αναφορά εκ μέρους του νομοθέτη για *«συνεκτίμηση των κριτηρίων».*[162] Επιπροσθέτως, στην παράγραφο 2 αναφέρεται ότι οι πάροχοι βασικών υπηρεσιών θα *λαμβάνουν «κατάλληλα μέτρα για αποτροπή και ελαχιστοποίηση του αντίκτυπου των συμβάντων, για τη διασφάλιση της συνέχειας του».*[163] Επομένως, και οι πάροχοι βασικών υπηρεσιών έχουν υποχρέωση αφενός να διασφαλίσουν την διαχείριση των κινδύνων και αφετέρου τη συνέχιση των υπηρεσιών που παρέχουν μέσω της αποτροπής και ελαχιστοποίησης των συνεπειών.[164]

Οι απαιτήσεις κοινοποίησης των παρόχων βασικών υπηρεσιών καθορίζονται στην στο άρθρο 16, παράγραφος 3. Σύμφωνα με την παράγραφο 3 «*οι πάροχοι ψηφιακών υπηρεσιών κοινοποιούν στην αρμόδια αρχή ή την CSIRT χωρίς αδικαιολόγητη καθυστέρηση κάθε συμβάν που έχει σημαντικό αντίκτυπο στην παροχή της υπηρεσίας που προσφέρουν εντός της Ένωσης, όπως αναφέρεται στο παράρτημα ΙΙΙ. Οι κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην αρμόδια αρχή ή την CSIRT να προσδιορίσουν τη σοβαρότητα τυχόν διασυνοριακού αντίκτυπου. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα».*[165]

Για τον προσδιορισμό ενός σημαντικού συμβάντος λαμβάνεται υπόψη «*α) ο αριθμός των χρηστών που επηρεάζονται από το συμβάν, ιδίως των χρηστών που*

[160] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

[161] Ibid *supra* 14, pp. 3-6.

[162] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

[163] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

[164] Ibid *supra* 14, pp. 3-6.

[165] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών· β) η διάρκεια του συμβάντος· γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν· δ) η έκταση της διατάραξης της λειτουργίας της υπηρεσίας· ε) η έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητες».[166] Οι παράμετροι θα πρέπει να εξεταστούν και εν προκειμένω σωρευτικά.

Από τα ανωτέρω, οι φορείς εκμετάλλευσης βασικών υπηρεσιών έχουν υποχρέωση κοινοποίησης όταν υπάρχει *«σοβαρός αντίκτυπος συμβάντος»* και οι πάροχοι βασικών υπηρεσιών έχουν υποχρέωση κοινοποίησης όταν υπάρχει «*σημαντικός αντίκτυπος συμβάντος*». Αν και η οδηγία θέτει ορισμένες παραμέτρους για τον προσδιορισμό της «σοβαρότητας» και του «σημαντικού» δεν παύουν οι έννοιες αυτές να παραμένουν αόριστες.[167] Οι παράμετροι της διαπίστωσης της *«σοβαρότητας»* επικαλύπτονται από την παράμετρο του *«σημαντικού»,* δημιουργώντας μια σύγχυση.[168] Οι πάροχοι βασικών υπηρεσιών υπόκεινται σε ήπιες απαιτήσεις, ιδίως αν ληφθεί υπόψη ότι σύμφωνα με την παράγραφο 4 του άρθρου 5 «*η υποχρέωση κοινοποίησης συμβάντος εφαρμόζεται μόνο σε περίπτωση που ο πάροχος ψηφιακών υπηρεσιών έχει πρόσβαση στις πληροφορίες που απαιτούνται για να εκτιμηθεί ο αντίκτυπος συμβάντος έναντι των παραμέτρων που αναφέρονται στο πρώτο εδάφιο».*[169] Ωστόσο, η ασάφεια των εννοιών ενδέχεται να προκαλέσει ανομοιομορφία στην εφαρμογή του ενωσιακού πλαισίου, καθώς τυχόν παραλείψεις κοινοποίησης των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων

[166] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

[167] Ibid *supra* 14, pp. 3-6.

[168] Ibid *supra* 14, pp. 3-6.

[169] Ibid *supra* 14, pp. 3-6.

ψηφιακών υπηρεσιών σύμφωνα με το άρθρο 21, μπορεί να οδηγήσει ορισμένα κράτη μέλη να επιβάλλουν κυρώσεις και άλλα όχι.[170]

Περαιτέρω, συγκριτικά με τις απαιτήσεις ασφάλειας και κοινοποίησης των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών, παρατηρείται ότι παρέχεται μεγαλύτερη ευελιξία στους τελευταίους να ενεργήσουν ελεύθερα.[171] Οι ελαφρύτερες απαιτήσεις προς τους παρόχους ψηφιακών υπηρεσιών διαπιστώνεται και μέσω των αιτιολογικών σκέψεων της οδηγίας. Συγκεκριμένα, σύμφωνα με την αιτιολογική σκέψη 49 «*οι απαιτήσεις ασφάλειας για τους παρόχους ψηφιακών υπηρεσιών θα πρέπει να είναι λιγότερο αυστηρές*».[172] Επιπροσθέτως, η αιτιολογική σκέψη 57 καταγράφει ότι «*η παρούσα οδηγία θα πρέπει να ακολουθήσει διαφοροποιημένη προσέγγιση όσον αφορά το επίπεδο εναρμόνισης για τις δύο αυτές ομάδες οντοτήτων. Όσον αφορά τους φορείς εκμετάλλευσης βασικών υπηρεσιών, τα κράτη μέλη θα πρέπει να έχουν τη δυνατότητα να προσδιορίζουν τους σχετικούς φορείς και να επιβάλλουν αυστηρότερες απαιτήσεις από αυτές που προβλέπονται στην παρούσα οδηγία».*[173] Τέλος, η αιτιολογική σκέψη 60 αναφέρει ότι *«οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να υπόκεινται σε ήπιες και αντενεργές εκ των υστέρων εποπτικές δραστηριότητες, δικαιολογούμενες από τη φύση των υπηρεσιών και των δραστηριοτήτων τους».*[174] Η διαφορετική προσέγγιση του ενωσιακού νομοθέτη, ως αναφέρθηκε και ανωτέρω, έγκειται στη διαφορετική φύση υπηρεσιών και δραστηριοτήτων που παρέχουν.[175]

---

[170] Ibid 108.

[171] Ibid *supra* 14, pp. 3-6.

[172] Ibid *supra* 50, Αιτιολογική Σκέψη 49 της Οδηγίας.

[173] Ibid *supra* 50, Αιτιολογική Σκέψη 57 της Οδηγίας.

[174] Ibid *supra* 50, Αιτιολογική Σκέψη 60 της Οδηγίας.

[175] Ibid *supra* 14, pp. 3-6.

Ως προς το ζήτημα των κυρώσεων, το άρθρο 21 της οδηγίας προβλέπει ότι *οι «προβλεπόμενες κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές».*[176] Αυτή η διάταξη έχει οδηγήσει τα κράτη μέλη να μεταφέρουν στο εσωτερικό τους την ως άνω πρόβλεψη με διαφορετικό τρόπο.[177] Για παράδειγμα το Βέλγιο και η Κύπρος πέραν από χρηματικές κυρώσεις, προβλέπουν και ποινές φυλάκισης.[178] Επιπλέον, το ύψος των κυρώσεων διαφέρει από κράτος μέλος σε κράτος πέλος.[179] Το ύψος των χρηματικών κυρώσεων κυμαίνεται σε διαφορετικά ύψη σε κάθε κράτος μέλος.[180] Επιπλέον, η Φιλανδία δεν προβλέπει κυρώσεις στον εναρμονιστικό της νόμου.[181]

Τα κράτη μέλη θα μπορούν να εξετάσουν αν οι οντότητες συμμορφώνονται με τις απαιτήσεις κυβερνοασφάλειας.[182] Οι επενδύσεις που θα γίνουν από τις οντότητες θα πρέπει να έχουν αποδοτικό χαρακτήρα, ήτοι το κόστος λήψης των προληπτικών μέτρων κατά των κινδύνων ή των μέτρων διαχείρισης των απειλών θα πρέπει να είναι χαμηλότερο από το κόστος των συνεπειών που ενδεχομένως να προκύψουν από την πραγμάτωση μιας επιτυχημένης κυβερνοεπίθεσης.[183] Τα κράτη μέλη εν προκειμένω, θα πρέπει να αξιολογήσουν αν τα μέτρα ασφάλειας είναι κατάλληλα. Οι ιδιωτικές επιχειρήσεις έχουν ως κίνητρο για την αποτελεσματική διασφάλιση των απαιτήσεων κυβερνοασφάλειας και την διαφύλαξη των ιδιωτικών τους συμφερόντων, π.χ. πλήξη της εμπορικής τους φήμη.[184] Επομένως μπορεί να επενδύσουν και σε δαπανηρά

[176] Ibid *supra* 50, Άρθρο 21 της Οδηγίας.

[177] Ibid *supra* 108.

[178] Ibid *supra* 108.

[179] Ibid *supra* 108.

[180] Ibid *supra* 108.

[181] Ibid *supra* 108.

[182] Ibid *supra* 143, pp. 28-29.

[183] Ibid *supra* 143, pp. 28-29

[184] Ibid *supra* 143, pp. 28-29

μέτρα. Ωστόσο η επένδυση σε δαπανηρά μέτρα δεν διασφαλίζει και την καταλληλόλητα των μέτρων προς το δημόσιο συμφέρον. Μπορεί δηλαδή οι οντότητες να πέσουν στην παγίδα και να πιστέψουν ότι το υψηλού κόστους σύστημα ασφάλειας είναι και αποτελεσματικό.[185] Εντούτοις, αυτό δεν συνεπάγεται ότι με τέτοια δαπανηρά μέτρα διασφαλίζεται και το ευρύτερο κοινωνικό συμφέρον.[186] Συνεπώς, θα πρέπει να παρέχονται επαρκή κίνητρα ιδίως προς τις ιδιωτικές οντότητες για τη λήψη των σωστών μέτρων.[187]

Επιπλέον, οι ιδιωτικές οντότητες ενδέχεται να μην κοινοποιήσουν τυχόν παραβιάσεις για να μην επηρεαστεί η φήμη τους.[188] Ως εκ τούτου, θα μπορούσε η οδηγία να δημιουργήσει ένα σύστημα ευθύνης για τα μέλη της διεύθυνσης των οντοτήτων που λόγω αμέλειας έλαβαν ακατάλληλα μέτρα που δεν διασφαλίζουν το κοινωνικό σύνολο και το ευρύτερο δημόσιο συμφέρον.[189] Αυτό θα ανάγκαζε τις οντότητες πέρα από το ζήτημα της αναλογικότητας των μέτρων, ήτοι κόστος επένδυσης ανάλογο των κινδύνων, να εξετάζει και την καταλληλόλητα των εν λόγω μέτρων όχι μόνο ως προς τις ενδεχόμενες συνέπειες στις εν λόγω οντότητες άλλα ευρύτερα και για το κοινωνικό σύνολο.[190] Αξιοσημείωτο είναι ότι έξι κράτη μέλη δεν καθορίζουν στους εναρμονιστικούς τους νόμους το είδος της αναγκαίας εποπτείας.[191]

[185] Ibid *supra* 143, pp. 28-29.

[186] Ibid *supra* 143, pp. 28-29.

[187] Ibid *supra* 143, pp. 28-29

[188] Ibid *supra* 143, pp. 28-29.

[189] Ibid *supra* 143, pp. 28-29.

[190] Ibid *supra* 143, pp. 28-29.

[191] Ibid *supra* 108.

ΙΙ. Η δύσκολη συνύπαρξη και συλλειτουργία Οδηγίας NIS και Κανονισμού GDPR

Οι υποχρεώσεις κοινοποίησης αναφοράς περιστατικών ασφάλειας που προβλέπει η Οδηγία NIS στους φορείς εκμετάλλευσης βασικών υπηρεσιών και στους παρόχους ψηφιακών υπηρεσιών διασφαλίζει την λογοδοσία τους ως προς την καταλληλόλητα και αναλογικότητα των μέτρων που λαμβάνουν σε περίπτωση παραβίασης των συστημάτων δικτύου και πληροφορίων. Ανάλογες υποχρεώσεις κοινοποίησης περιστατικών ασφάλειας, προβλέπει ο νομοθέτης της Ένωσης και σε άλλα νομοθετικά κείμενα, όπως στο άρθρο 19 (2) του Κανονισμού 910/2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά, στο άρθρο 96 στην Οδηγία 2015/23/66/ΕΕ σχετικά με τις υπηρεσίες πληρωμών στην εσωτερική αγορά και στο άρθρο 40(2) της Οδηγίας 2018/1972 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών.[192] Κατ' αυτόν τον τρόπο ο ενωσιακός νομοθέτης παρεμβαίνει καθορίζοντας τις απαιτήσεις κοινοποίησης σε διάφορούς τομείς και ως προς διαφορετικές οντότητες με απώτερο στόχο την προστασία της εσωτερικής αγοράς της Ένωσης από τους ενδεχόμενους για τον κυβερνοχώρο κινδύνους.[193] Συνεπώς, η κοινοποίηση αναφοράς περιστατικών παρατηρείται και σε άλλα νομοθετικά κείμενα της Ένωσης, λόγω της υιοθέτησης των πληροφοριακών συστημάτων σχεδόν σε όλους τους τομείς της ανθρώπινης δραστηριότητας γεγονός

[192] Sandra Schmitz-Berndt, Stephen Schiffner, «Don't Put the Cart Before the Horse – Effective Incident Handling Under GDPR and NIS Directive», *IFIP International Summer School on Privacy and Identity Management,* Privacy and Identity, 2020, pp 4.

[193] Ibid supra 24, pp. 101-102.

που έχει ως αποτέλεσμα να καλύπτονται πρόσθετοι τομείς και να επιβάλλονται ανάλογες υποχρεώσεις και σε διαφορετικές οντότητες ανά περίπτωση.[194]

Σύμφωνα με το άρθρο 1 παράγραφος 3 από το πεδίο εφαρμογής της οδηγίας NIS εξαιρούνται οι *«επιχειρήσεις που υπόκεινται στις απαιτήσεις των άρθρων 13α και 13β της οδηγίας 2002/21/ΕΚ ή σε παρόχους υπηρεσιών εμπιστοσύνης που υπόκεινται στις απαιτήσεις του άρθρου 19 του κανονισμού (ΕΕ) αριθ. 910/2014».*[195] Επομένως, τα ως άνω νομοθετικά κείμενα της Ένωσης εξαιρούνται από το πεδίο εφαρμογής της Οδηγίας NIS εφόσον οι απαιτήσεις ασφάλειας κρίνεται ότι διασφαλίζονται από αυτά επαρκώς. Επιπροσθέτως, η παράγραφος 7 του άρθρου 1 της οδηγίας, ορίζει ότι όταν μια νομοθετική πράξη της Ένωσης προβλέπει είτε παρόμοιες απαιτήσεις ασφάλειας είτε παρόμοιες απαιτήσεις κοινοποίησης, οι οποίες έχουν ισοδύναμο αποτελέσμα με αυτό της οδηγίας NIS, τότε και θα εφαρμόζονται και οι διατάξεις της εν λόγω πράξης ως lex specialis. Χαρακτηριστικό, παράδειγμα αποτελεί το άρθρο 96 στην Οδηγία 2015/23/66/ΕΕ.[196]

Εντούτοις, παρόμοιες υποχρεώσεις προβλέπονται και στον Κανονισμό 2016/679 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (εφεξής Κανονισμός GDPR).[197] Ο Κανονισμός GDPR έχει ως κύριο σκοπό την προστασία των φυσικών προσώπων και ειδικότερα της ιδιωτικής

[194] Ibid supra 24, pp. 101-102.

[195] Ibid supra 50, Άρθρο 1 της Οδηγίας.

[196] Ibid supra 24, pp. 104-105.

[197] Sandra Schmitz-Berndt, Stephan Schiffner, « Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR», *International Review of Law*, Computers & Technology, 2021, Vol 35, No. 2, pp.101-102

ζωής τους μέσω της διαφύλαξης των προσωπικών τους δεδομένων.[198] Ο Κανονισμός θέτει απαιτήσεις ασφάλειας έναντι της επεξεργασίας που μπορεί να τυγχάνουν τα προσωπικά δεδομένα των φυσικών προσώπων και διασφαλίζει την ελεύθερη κυκλοφορία τέτοιων δεδομένων εντός της Ένωσης.[199] Περαιτέρω, ο εν λόγω Κανονισμός απαιτεί σε περιπτώσεις παραβιάσεις των προσωπικών δεδομένων των φυσικών προσώπων να κοινοποιούνται οι εν λόγω παραβιάσεις τους αρμόδιους εποπτικούς φορείς και στα υποκείμενα των προσωπικών δεδομένων που παραβιαστήκαν.[200] Σε περίπτωση μη συμμόρφωσης με τις απαιτήσεις ασφάλειας και κοινοποίησης των περιστατικών, ο ανωτέρω Κανονισμός επιβάλλει σχετικές κυρώσεις.[201]

Εκ των ανωτέρων στοιχείων, το ερώτημα που ανακύπτει είναι κατά πόσο οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται στον Κανονισμό GDPR μπορούν να θεωρηθούν ως lex specialis της Οδηγίας NIS κατ' εφαρμογή του άρθρου 1 της παραγράφου 7 της οδηγίας NIS.[202] Τα δυο αυτά νομοθετικά κείμενα έχουν ως σκοπό την διασφάλιση της ασφάλειας των συστημάτων τεχνολογίας πληροφορίων και των δεδομένων που αποτελούν αντικείμενο επεξεργασίας από τα εν λόγω συστήματα.[203] Επομένως, σκοπός του νομοθέτη της Ένωσης ήταν η θέσπιση δύο πράξεων για τη διασφάλιση της λειτουργίας της εσωτερικής αγοράς της Ένωσης.[204]

---

[198] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679

[199] Ibid 198.

[200] Ibid *supra* 197, pp. 101-102.

[201] Ibid *supra* 40, pp. 7-8.

[202] Ibid *supra* 24, pp. 104-105.

[203] Ibid *supra* 197, pp. 101-102.

[204] Ibid *supra* 197, pp. 101-102.

Με την Οδηγία NIS διασφαλίζεται η παροχή υπηρεσιών εκ μέρους των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών και με τον Κανονισμό GDPR η διασφάλιση των προσωπικών δεδομένων που βρίσκονται τις υπηρεσίες των ανωτέρων[205]. Ωστόσο, η οδηγία NIS εστιάζει στην αυτοματοποιημένη επεξεργασία ψηφιακών δεδομένων στα συστήματα δικτύων και πληροφορίων. Επομένως, από το πεδίο εφαρμογής της προκύπτει ότι δεν εμπίπτουν σε αυτό μη ψηφιακές πληροφορίες.[206] Αν και τα δυο νομοθετικά κείμενα καθορίζουν απαιτήσεις ασφάλειας και κοινοποίησης, καθώς και κυρώσεις σε περίπτωση μη συμμόρφωσης δεν θα μπορούσε ο Κανονισμός GDPR να θεωρηθεί ως lex specialis της Οδηγίας, αφενός επειδή ο σκοπός του κάθε κειμένου είναι διαφορετικός και αφετέρου επειδή οι αρμόδιες αρχές που θα ειδοποιηθούν είναι διαφορετικές.[207]

Ωστόσο, υπάρχουν περιπτώσεις που τα δύο κείμενα μπορούν να εφαρμόζονται παράλληλα. Σε αυτή την περίπτωση δεν υπάρχει κάποια ρητή αναφορά στην εφαρμογή του ενός κειμένου στο άλλο.[208] Αυτό έχει ως αποτέλεσμα να μην είναι δεσμευτικό το κείμενο του ενός για το άλλο. Κατά την εφαρμογή και των δύο πράξεων υπάρχουν ορισμένες κοινές υποχρεώσεις (Α), ωστόσο παρατηρείται και μια ασάφεια ως προς τις κοινές υποχρεώσεις (Β). Οι ασάφειες έγκεινται κυρίως στο γεγονός ότι ο νομοθέτης αναφορικά με την προστασία των προσωπικών δεδομένων επιλέγει την θέσπιση ενός κανονισμού, ο οποίος έχει άμεσο και καθολικό αποτέλεσμα.[209] Ενώ ως προς την ασφάλεια των συστημάτων δικτύου και πληροφορίων επιλέγει τη θέσπιση μιας Οδηγίας, την οποία τα κράτη μέλη θα

[205] Ibid *supra* 197, pp. 101-102.

[206] Rogers Alunge, «Breach of security vs personal data breach: effect on EU data subject notification requirements», *International Data Privacy Law*, Volume 11, Issue 2, April 2021, pp. 171.

[207] Ibid *supra* 24, pp. 104-105.

[208] Ibid *supra* 14, pp. 9-11.

[209] Ibid *supra* 14, pp. 9-11.

μπορούν να μεταφέρουν στο εσωτερικό της έννομης τους τάξη με βάση τις δικές τους ανάγκες.[210] Επομένως, η οδηγία παρέχει μεγαλύτερη ευχέρεια στα κράτη μέλη να καθορίσουν τον τρόπο εναρμόνισης του περιεχομένου της οδηγίας.[211] Αυτό το γεγονός οδηγεί πιθανότατα σε μια ανομοιομορφία. Θα εξετάσουμε στη συνέχεια τα σημεία σύγκρουσης ορισμένων διατάξεων των δυο αυτών νομοθετικών κειμένων(Γ).

(Α) Οι Κοινές εν μέρει προσεγγίσεις προς τις αρμόδιες αρχές

Το πρώτο σημείο αλληλεπίδρασης των κειμένων εντοπίζεται όταν τα προσωπικά δεδομένα των φυσικών προσώπων βρίσκονται στα συστήματα των φορέων εκμετάλλευσης βασικών υπηρεσιών είτε στα συστήματα των παρόχων ψηφιακών υπηρεσιών.[212] Το ερώτημα επομένως που τίθεται είναι εάν οι απαιτήσεις ασφάλειας που θεσπίζονται στην Οδηγία NIS είναι ικανοποιητικές ή και επαρκείς σε σχέση με τις απαιτήσεις του Κανονισμού GDPR και αντιστρόφως.[213]

Η Οδηγία NIS απαιτεί από τους φορείς εκμετάλλευσης βασικών υπηρεσιών (άρθρο 14, παράγραφος 1) και από τους παρόχους ψηφιακών υπηρεσιών (άρθρο 16, παράγραφος 1) να λαμβάνουν «*κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων*».[214] Οι έννοιες «*κατάλληλα και αναλογικά*» και «*τεχνικά και οργανωτικά μέτρα»* δεν ερμηνεύονται περαιτέρω παρέχοντας τους ευρεία διακριτική ευχέρεια ως προς τα απαιτούμενα μέτρα που μπορούν να ληφθούν.[215] Παράλληλα, ο Κανονισμός GDPR προβλέπει στο άρθρο 32 ότι *«ο υπεύθυνος*

[210] Ibid *supra* 14, pp. 9-11.

[211] Ibid *supra* 14, pp. 9-11.

[212] Ibid *supra* 14, pp. 9-11.

[213] Ibid *supra* 14, pp. 9-11.

[214] Ibid *supra* 14, pp. 9-11.

[215] Ibid *supra* 14, pp. 9-11.

επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων»[216]. Εκ των ανωτέρω, συνάγεται ότι παρέχονται κοινά μέτρα με σκοπό την επίτευξη της απαιτούμενης ασφάλειας και στα δύο νομοθετικά κείμενα. Εντούτοις, ο Κανονισμός GDPR αναφορικά με την απόδειξη της συμμόρφωσης του υπευθύνου επεξεργασίας και του εκτελούντα την επεξεργασία προβλέπει ειδικότερα στο άρθρο 40 έναν εγκεκριμένο κώδικα δεοντολογίας βάσει του οποίου μπορούν να δράσουν και στο άρθρο 42 ένα εγκεκριμένο μηχανισμό πιστοποίησης.[217] Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία ενεργούν δυνάμει ενός πλαισίου που καθορίζεται σαφώς εντός του Κανονισμού.[218]

Επιπροσθέτως και τα δύο νομοθετικά κείμενα θεσπίζουν υποχρεώσεις κοινοποίησης αναφοράς περιστατικών ασφάλειας.[219] Η υποχρέωση κοινοποίησης θεωρείται ως μέτρο αντιμετώπισης και πρόληψης και στα δύο νομοθετικά κείμενα.[220] Ειδικότερα, στην Οδηγία NIS επιβάλλεται η κοινοποίηση των περιστατικών σε *«κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός» που* δύναται να έχει *«δυνητική δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών»*[221]. Η υποχρέωση αυτή βαραίνει τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών. Οι υποχρεώσεις μεταξύ των δύο οντοτήτων διαφέρουν. Οι φορείς εκμετάλλευσης βασικών υπηρεσιών οφείλουν να κοινοποιήσουν *«χωρίς αδικαιολόγητη καθυστέρηση»* στην αρμόδια εθνική αρχή (NCA) ή την ομάδα

[216] Ibid *supra* 198, Άρθρο 32 του Κανονισμού.

[217] Lazaros Grigoriadis, «Cybersecurity Insurance and New EU Cybersecurity and Data Protection Rules», *Business Law Review*, 2017, Vol. 38 Issue 6, pp. 214.

[218] Ibid 217.

[219] Ibid *supra* 197, pp. 101-102.

[220] Ibid *supra* 192, pp. 1-2

[221] Ibid *supra* 50, Άρθρο 4 της Οδηγίας (ορισμός κινδύνου).

αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (SCRT) κάθε περιστατικό που έχει σοβαρό αντίκτυπο στην ασφάλεια των συστημάτων πληροφορίων και δικτύων.[222] Αντίστοιχα, οι πάροχοι ψηφιακών υπηρεσιών οφείλουν να κοινοποιήσουν «χωρίς αδικαιολόγητη καθυστέρηση» στην αρμόδια εθνική αρχή (NCA) ή την ομάδα αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (SCRT) κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην ασφάλεια των συστημάτων πληροφορίων και δικτύων.[223]

Η έννοια του σοβαρού περιστατικού προσδιορίζεται μέσω ορισμένων παραμέτρων που καθορίζει το άρθρο 14 παράγραφος 4 και η έννοια και του σημαντικού αντίκτυπου προσδιορίζεται μόνο βάσει ορισμένων παραμέτρων που καθορίζει η παράγραφος 4 του άρθρου 16.[224] Επιπροσθέτως, ο Κανονισμός 2018/15120 καθορίζει ορισμένες πρόσθετες παραμέτρους που δύναται να ληφθούν υπόψη στην περίπτωση σημαντικού αντικτύπου, όπως να έχουν επηρεαστεί πέραν των 100.000 χρηστών ή και η ζημία που προκλήθηκε να υπερβαίνει το 1.000.0000 ευρώ.[225] Επιπροσθέτως, ακόμη μια διαφοροποίηση μεταξύ των δύο οντοτήτων, ήτοι τους φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών, έγκειται στο γεγονός ότι οι τελευταίοι η υποχρέωση κοινοποίησης αφορά μόνο όποιον *«έχει πρόσβαση στις πληροφορίες που απαιτούνται για να εκτιμηθεί ο αντίκτυπος συμβάντος»*.[226]

Ο Κανονισμός GDPR επιβάλλει στους υπευθύνους επεξεργασίας δεδομένων την υποχρέωση κοινοποίηση των περιστατικών παραβιάσεις προσωπικών δεδομένων

[222] Ibid *supra* 24, pp. 102-103.

[223] Ibid *supra* 24, pp. 102-103.

[224] Ibid *supra* 24, pp. 102-103.

[225] Ibid *supra* 24, pp. 102-103.

[226] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

σε δυο περιπτώσεις.[227] Η πρώτη περίπτωση αφορά την υποχρέωση κοινοποίησης στις αρμόδιες εποπτικές αρχές (άρθρο 33) και η δεύτερη περίπτωση στην ενημέρωση των υποκειμένων των προσωπικών δεδομένων (άρθρο 34).[228] Ειδικότερα, σύμφωνα με το άρθρο 33 του Κανονισμού ο «*εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας αμελλητί, μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα»* και αντίστοιχα *«ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια».*[229] Επιπροσθέτως, το άρθρο 33 προβλέπει ότι *«όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση».*[230]

Επιπροσθέτως, ο Κανονισμός GDPR στο άρθρο 33, παράγραφος 3, επιτάσσει κατά την κοινοποίηση των περιστατικών να παρέχονται ορισμένες πληροφορίες. Πρέπει η κοινοποίηση κατ' ελάχιστο να *«(α) περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα, β) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες, γ)περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα, δ) περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον*

[227] Ibid *supra* 192, pp. 6, 10.

[228] Ibid *supra* 24, pp. 103.

[229] Ibid *supra* 198, Άρθρο 33 του Κανονισμού.

[230] Ibid *supra* 198, Άρθρο 33 του Κανονισμού.

υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της».[231]

Συγκρίνοντας τα δύο νομοθετικά κείμενα ως προς τις υποχρεώσεις κοινοποίησης δημιουργούνται ορισμένοι προβληματισμοί. Πρώτον, η φράση *«χωρίς αδικαιολόγητη καθυστέρηση»* δεν ερμηνεύεται περαιτέρω στην Οδηγία NIS. Αυτό έχει ως συνέπεια τα κράτη μέλη να ακολουθήσουν διαφορετικές προσεγγίσεις κατά την ενσωμάτωση των σχετικών διατάξεων.[232] Για παράδειγμα, το Ηνωμένο Βασίλειο καθορίζει αυτό το χρονικό πλαίσιο προβλέποντας ότι η κοινοποίηση πρέπει να γίνει *«εντός των 72 ωρών»* ενώ η Εσθονία *«το αργότερο εντός 24 ωρών»*.[233] Αντίθετα τα υπόλοιπα κράτη φαίνεται να υιοθετούν την αόριστη έννοια της *«αδικαιολόγητης καθυστέρησης»*.[234] Η διαφορετική προσέγγιση των κρατών μελών ενδέχεται να οδηγήσει σε μια ανομοιομορφία μεταξύ των κρατών μελών. Αντίθετα ο Κανονισμός GDPR προσδιορίζει το χρονικό πλαίσιο κοινοποίησης στην αρμόδια εποπτική αρχή.[235] Το χρονικό πλαίσιο είναι ενιαίο και ομοιόμορφο και κάθε κράτος μέλος θα πρέπει να συμμορφωθεί προς αυτό. Συνεπώς, σε περίπτωση που τα προσωπικά δεδομένα των φυσικών προσώπων που βρίσκονται είτε στα συστήματα των φορέων εκμετάλλευσης βασικών υπηρεσιών είτε στα συστήματα των παρόχων ψηφιακών υπηρεσιών παραβιαστούν, οι φορείς εκμετάλλευσης βασικών υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών μπορεί να μην ενεργήσουν εντός του χρονικού

[231] Ibid *supra* 198, Άρθρο 33 του Κανονισμού.

[232] Ibid *supra* 197, pp. 104.

[233] Ibid *supra* 197, pp. 104.

[234] Ibid *supra* 197, pp. 104.

[235] Ibid *supra* 197, pp. 104.

διαστήματος που επιτάσσει ο Κανονισμός GDPR.[236] Ωστόσο, όπως προαναφέρθηκε ανωτέρω, αν δεν ενημερωθούν οι εποπτικές αρχές εντός της προβλεπόμενης προθεσμίας θα πρέπει να αιτιολογήσουν ως προς την καθυστέρηση. Ο δεύτερος προβληματισμός έγκειται στο γεγονός ότι οι υπεύθυνοι επεξεργασίας δεδομένων υποχρεούνται να παράσχουν στις αρμόδιες εποπτικές αρχές ορισμένες de minimis πληροφορίες. Ως εκ τούτου, ένα περιστατικό που μπορεί να ενεργοποιήσει την εφαρμογή των νομοθετικών κειμένων ενέχει τον κίνδυνο να αντιμετωπιστεί ως δυο διαφορετικά περιστατικά λόγω των διαφορετικών χρονικών πλαισίων κοινοποιήσης άλλα και λόγω του γεγονότος ότι οι εποπτικές αρχές του Κανονισμού GDPR θα έχουν μια πιο εμπεριστατωμένη εικόνα του περιστατικού από αυτή των αρμόδιων αρχών της Οδηγίας NIS.

Σε αυτές στις περιπτώσεις, το άρθρο 15, παράγραφος 4, της Οδηγίας NIS αναφέρει ότι *«κατά την αντιμετώπιση συμβάντων που οδηγούν σε παραβιάσεις προσωπικών δεδομένων, η αρμόδια αρχή συνεργάζεται στενά με τις αρχές προστασίας δεδομένων».*[237] Επομένως, για να μην αντιμετωπιστεί ένα περιστατικό ως δυο διαφορετικά οι αρμόδιες αρχές της οδηγίας NIS και οι εποπτικές αρχές του Κανονισμού GDPR θα πρέπει να συνεργαστούν και να ανταλλάξουν πληροφορίες. Η διάταξη είναι επιχείρημα υπέρ της θέσης ότι τα δύο νομοθετικά κείμενα αυτά θα πρέπει να ενεργούν συμπληρωματικά.[238]

[236] Ibid *supra* 197, pp. 104-106.

[237] Ibid *supra* 50, Άρθρο 15 της Οδηγίας.

[238] Ibid *supra* 197, pp. 111-112.

(Β) Διαφορετικές προσεγγίσεις ως προς την ενημέρωση του κοινού και των επηρεαζόμενων

Η Οδηγία NIS δεν προβλέπει στο κείμενο της τη δυνατότητα ενημέρωσης των ατόμων που έχουν επηρεαστεί από ένα περιστατικό. Ωστόσο, ορίζει τη δυνατότητα ενημέρωσης του κοινού σε ορισμένα μεμονωμένα περιστατικά.[239] Ειδικότερα στην περίπτωση των φορέων εκμετάλλευσης βασικών υπηρεσιών, το άρθρο 14, παράγραφος 4, αναφέρει ότι *«η αρμόδια αρχή ή η CSIRT μπορεί να ενημερώνει το κοινό σχετικά με μεμονωμένα συμβάντα, σε περίπτωση που η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη».*[240] Επιπροσθέτως, στην περίπτωση των παρόχων ψηφιακών υπηρεσιών σύμφωνα το άρθρο 16, παράγραφος 7 ορίζεται ότι *«η αρμόδια αρχή ή η CSIRT και, κατά περίπτωση, οι αρχές ή οι CSIRT άλλων ενδιαφερομένων κρατών μελών μπορούν να ενημερώνουν το κοινό σχετικά με μεμονωμένα συμβάντα ή να απαιτούν από τον πάροχο ψηφιακών υπηρεσιών να το πράξει, όταν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη ή σε περίπτωση που η αποκάλυψη του συμβάντος είναι προς το δημόσιο συμφέρον».*[241]

Επιπροσθέτως, η αιτιολογική σκέψη 59 της Οδηγίας NIS αναφέρει ότι η κοινοποίηση προς το κοινό μπορεί να ανασταλεί με σκοπό την εξισορρόπηση του ενδιαφέροντος του κοινού με την πιθανή βλάβη στη φήμη που μπορεί να προκαλέσει η δημοσιοποίηση με τέτοιας βλάβης στους παρόχους ψηφιακών υπηρεσιών και στους

[239] Ibid *supra* 24, pp.105.

[240] Ibid *supra* 50, Άρθρο 14 της Οδηγίας.

[241] Ibid *supra* 50, Άρθρο 16 της Οδηγίας.

φορείς εκμετάλλευσης βασικών υπηρεσιών.[242] Από την ανωτέρω, αιτιολογική σκέψη συνάγεται ότι τα επιχειρηματικά συμφέροντα των ανωτέρω οντοτήτων τυγχάνουν ίσης προστασίας με το συμφέρον του κοινού για ενημέρωση περιστατικών ασφαλείας.

Ο Κανονισμός GDPR επιτάσσει δυνάμει του άρθρου 34 τον υπεύθυνο επεξεργασίας δεδομένων *«να ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα»* στο υποκείμενο των δεδομένων «*όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».*[243] Η κοινοποίηση αυτή του υπευθύνου επεξεργασίας σύμφωνα με το άρθρο 34 παράγραφος 2, θα πρέπει να περιγράφει με σαφήνεια *«τη φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα»* και να δίνονται «δ*τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ)».*[244] Η μόνη διαφοροποίηση μεταξύ της κοινοποίησης στις αρμόδιες εποπτικές αρχές (άρθρο 33) και στα υποκείμενα των δεδομένων (άρθρο 34) έγκειται στο είδος του κινδύνου, ήτοι ως προς το αν ο κίνδυνος είναι υψηλός ή οχι.[245] Ειδικότερα, η αιτιολογική σκέψη 76 του Κανονισμού GDPR αναφέρει ότι *«ο κίνδυνος θα πρέπει να αξιολογείται βάσει αντικειμενικής εκτίμησης, με την οποία διαπιστώνεται κατά πόσον οι πράξεις επεξεργασίας δεδομένων συνεπάγονται κίνδυνο ή υψηλό κίνδυνο»*.[246]

Η υποχρέωση κοινοποίησης στα υποκείμενα των δεδομένων δυνάμει του Κανονισμού GDPR δεν είναι απόλυτη. Υπάρχουν περιπτώσεις στις οποίες δύναται να

[242] Ibid *supra* 50, Αιτιολογική Σκέψη 59 της Οδηγίας.

[243] Ibid *supra* 198, Άρθρο 34 του Κανονισμού.

[244] Ibid *supra* 198, Άρθρο 34 του Κανονισμού.

[245] Ibid *supra* 24, pp. 103-105.

[246] Ibid *supra* 198, Αιτιολογική Σκέψη 76 του Κανονισμού.

μην ενημερωθεί το υποκείμενο παρά τον υψηλό κίνδυνο που διατρέχουν τα προσωπικά τους δεδομένα. Οι περιπτώσεις αυτές καθορίζονται στο άρθρο 34 παράγραφος 2 και αφορά τις ακόλουθες περιπτώσεις.[247] Πρώτον, αφορά την περίπτωση όπου ο *«υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα»,* όπως για παράδειγμα να ήταν κρυπτογραφημένα και ως εκ τούτου μη κατανοητά με σκοπό την επεξεργασία τους.[248] Δεύτερον αφορά την περίπτωση όπου «*ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει»* ο όποιος υψηλός κίνδυνος στα δικαιώματα και τις ελευθερίες των υποκείμενων δεδομένων.[249] Τρίτον, όταν η εν λόγω κοινοποίηση «*προϋποθέτει δυσανάλογες προσπάθειες».*[250] Σε αυτήν την περίπτωση, επιτρέπεται η δημόσια ανακοίνωση ή παρόμοιο μέτρο εξίσου αποτελεσματικό.[251]

(Γ) Σημεία Σύγκρουσης των διατάξεων

Ένα σημείο σύγκρουσης των δύο νομοθετικών πράξεων υφίσταται όταν δυνάμει της Οδηγίας NIS οι πάροχοι ψηφιακών υπηρεσιών ή οι φορείς εκμετάλλευσης βασικών υπηρεσιών επιθυμούν την καθυστέρηση κοινοποίησης με σκοπό την περαιτέρω εξέταση που αντικτύπου και των ενδεχομένων περαιτέρω συνέπειων.[252] Το ερώτημα που τίθεται είναι εάν η άμεση ειδοποίηση των υποκειμένων μπορεί να μην διενεργηθεί με σκοπό το γενικό συμφέρον της ασφάλειας

[247] Ibid *supra* 192, pp. 6-13.

[248] Ibid *supra* 198, Άρθρο 34 του Κανονισμού.

[249] Ibid *supra* 198, Άρθρο 34 του Κανονισμού.

[250] Ibid *supra* 198, Άρθρο 34 του Κανονισμού.

[251] Ibid *supra* 24, pp. 104.

[252] Ibid *supra* 192, pp. 8-9.

των πληροφοριών.[253] Στον Κανονισμό GDPR τα υποκείμενα πρέπει να ενημερώνονται με σκοπό την προφύλαξη των δεδομένων τους ή τον περιορισμό των επιπτώσεων (π.χ. κλοπή ταυτότητας, οικονομική απώλεια λόγω πρόσβασης σε στοιχεία τραπεζικού λογαριασμού κ.α.).[254] Εντούτοις, οι πάροχοι ψηφιακών υπηρεσιών και οι φορείς εκμετάλλευσης βασικών υπηρεσιών για σκοπούς μετριασμού του αντίκτυπου και των επιπτώσεων μπορεί να επιθυμούν να μην δημοσιοποιηθεί η παραβίαση άμεσα.[255]

Το άρθρο 23 του Κανονισμού GDPR ορίζει ότι η υποχρέωση που παρέχεται στο άρθρο 34 του Κανονισμού, ήτοι για ενημέρωση των υποκειμένων αναφορικά με την παραβίαση των προσωπικών τους δεδομένων, δύναται να περιοριστεί όταν ένας «*τέτοιος περιορισμός σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση της δημόσιας ασφάλειας»,* εκτός αν ο εν λόγω περιορισμός αποβεί επιζήμιος προς το υποκείμενο.[256] Η ως άνω διάταξη θα μπορούσε να τύχει εφαρμογής με σκοπό την καθυστέρηση ενημέρωσης των επηρεαζόμενων για σκοπούς μετριασμού των ενδεχόμενων συνεπειών από τους παρόχους ψηφιακών υπηρεσιών ή τους φορείς εκμετάλλευσης βασικών υπηρεσιών με αναφορά προς το γενικό συμφέρον του κυβερνοχώρου στην Ένωση. Η ενεργοποίηση της ως άνω διάταξης θα πρέπει να ασκείται με ιδιαίτερη φειδώ, καθώς υπάρχουν περιπτώσεις που μπορεί ένα συμβάν να προέρχεται από ανθρώπινο λάθος ή τυχαίο γεγονός.[257] Επιπροσθέτως, εν

[253] Ibid *supra* 192, pp. 8-9.

[254] Ibid *supra* 217, pp. 214.

[255] Ibid *supra* 192, pp. 8-9.

[256] Ibid *supra* 198, Άρθρο 23 του Κανονισμού.

[257] Ibid *supra* 192, pp. 12-13.

τοις πράγμασι είναι δύσκολο σε αυτές τις περιπτώσεις να γίνει εκ των προτέρων η επίκληση των ανωτέρω με σκοπό τη μη κοινοποίηση προς τα υποκείμενα.[258]

Η αιτιολογική σκέψη 63 της Οδηγίας NIS αναφέρει ότι σε περιπτώσεις παραβίασης προσωπικών δεδομένων οι αρμόδιες αρχές της παρούσας οδηγίας *«και οι αρχές προστασίας δεδομένων πρέπει να συνεργάζονται και να ανταλλάσσουν πληροφορίες για όλα τα συναφή θέματα με σκοπό την αντιμετώπιση των παραβιάσεων δεδομένων προσωπικού χαρακτήρα οι οποίες οφείλονται σε συμβάντα».*[259] Κατ' αυτόν τον τρόπο τα δυο νομοθετικά αυτά κείμενα μπορούν να ενεργούν συμπληρωματικά και να αντιμετωπίζουν κάθε περιστατικό μέσω ανταλλαγής πληροφοριών. Ωστόσο δεν υπάρχει οποιαδήποτε νομική υποχρέωση που να διασφαλίζει την εν λόγω συμπληρωματικότητα των δύο νομοθετικών κειμένων.[260] Μέσω της συστηματικής εξέτασης των ανωτέρω νομοθετικών κειμένων διαπιστώνεται η ανάγκη άμεσης συνεργασίας των αρμόδιων αρχών που προβλέπονται από αυτά. Η απλή γενική επιθυμία για συνεργασία δεν αρκεί.[261] Απαιτείται πρόβλεψη νομικής υποχρέωσης συστηματικής συνεργασία, η οποία απουσιάζει από τα υφιστάμενα κείμενα των δύο πράξεων.[262] Η Ομάδα Συνεργασία της NIS στη δημοσίευση 04/20 αναφέρεται στην έλλειψη συνεργασίας των εμπλεκόμενων αρχών και στην απροθυμία ως προς την ανταλλαγή πληροφοριών.[263] Γι' αυτό και αναφέρεται στην ανάγκη ευθυγράμμισης των υποχρεώσεων κοινοποίησης περιστατικών στα δύο αυτά νομοθετικά κείμενα.[264]

[258] Ibid *supra* 192, pp. 12-13.

[259] Ibid *supra* 50, Αιτιολογική Σκέψη 63 της Οδηγίας.

[260] Ibid *supra* 192, pp. 14.

[261] Ibid *supra* 192, pp. 14.

[262] Ibid *supra* 192, pp. 14.

[263] Ibid *supra* 24, pp. 105.

[264] Ibid *supra* 24, pp. 105.

Τα πορίσματα της δημοσίευσης αυτής της Ομάδας Συνεργασίας εντάσσονται στην πρόταση για αναθεώρηση της υπάρχουσας οδηγίας NIS.[265]

III. Οι επερχόμενες αλλαγές μετά την πρόταση για αναθεώρηση της Οδηγίας NIS

Δύο χρόνια μετά την εφαρμογή της Οδηγίας NIS, η Επιτροπή και ο Ύπατος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας ανακοίνωσαν τη νέα στρατηγική της Ένωσης για διαμόρφωση ενός ψηφιακού μέλλοντος της Ένωσης για συλλογική ανθεκτικότητα και αυτονομία έναντι των κυβερνοαπειλών.[266] Στις 16/12/2020 η Ευρωπαϊκή Επιτροπή υπέβαλε πρόταση για αναθεώρηση της οδηγίας NIS.[267] Στην αιτιολογική της πρόταση αναφέρεται στην αναγκαιότητα κατάργησης της υφιστάμενης οδηγίας και θέσπισης μιας νέας ρύθμισης που θα προβλέπει έναν καθολικό και αποτελεσματικό μηχανισμό συνεργασίας στον κυβερνοχώρο.[268] Η πρόταση εξηγεί τους λόγους τροποποίησης του υφιστάμενου νομοθετικού πλαισίου σημειώνοντας την αυξανόμενη ψηφιοποίηση της εσωτερικής αγοράς άλλα και τις συνεχείς απειλές στον κυβερνοχώρο, οι οποίες ενισχύθηκαν περαιτέρω με την έναρξη της πανδημίας COVID-19.[269] Η πανδημία έφερε στο προσκήνιο τις σημαντικές αδυναμίες εφαρμογής της Οδηγίας NIS λόγω της άμεσης ανάγκης για ψηφιοποίηση της οικονομίας και της ευρύτερης κοινωνικής ζωής.[270]

[265] Mark D. Cole, «Recent developments and overview of the country and practitioner's reports», *European Data Protection Law Review (EDPL)*, 2021, Vol 7, No. 1, pp. 93.

[266] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[267] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[268] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[269] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[270] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

Η Επιτροπή αναγνωρίζει αφενός ότι η Οδηγία NIS συνιστά σημαντικό επίτευγμα για την εσωτερική αγορά της Ένωσης καθότι συνέβαλε στη θέσπιση εθνικών στρατηγικών κυβερνοασφάλειας στα κράτη μέλη, στην ενίσχυση της συνεργασίας μεταξύ τους και στη βελτίωση της ανθεκτικότητας σε επτά φορείς εκμετάλλευσης βασικών υπηρεσιών (ενέργεια, μεταφορές, τράπεζες, υποδομές χρηματοπιστωτικών αγορών, υγειονομική περίθαλψη, παροχή, διανομή πόσιμου νερού και ψηφιακές υποδομές), καθώς και σε τρείς παρόχους ψηφιακών υπηρεσιών (επιγραμμικές αγορές, επιγραμμικές μηχανές αναζήτησης και υπηρεσίες νεφοϋπολογιστική) μέσω των απαιτήσεων για αυξημένη ασφάλεια και αναφορά των σημαντικών ή σοβαρών περιστατικών.[271] Παρ' όλα ταύτα, η Επιτροπή συμμερίζεται και τις εγγενείς αδυναμίες και περιορισμούς ορισμένων διατάξεων της Οδηγία NIS κατά την μεταφορά και την εφαρμογή της από τα κράτη μέλη, όπως αυτά προκύπτουν μετά από δύο χρόνια πρακτικής εφαρμογής.

Προς υποστήριξη της παρέμβασής της, η Επιτροπή επικαλείται πρώτον, το περιοριστικά προσδιορισμένο πεδίο εφαρμογής της οδηγίας NIS.[272] Το ιδιαίτερα στενά πεδίο εφαρμογής είναι μια από τις σημαντικές αδυναμίες της ενόψει της αυξημένης ψηφιοποίησης.[273] Ειδικότερα, αναφέρει στην πρόταση της ότι δεν καλύπτονται εντός του πεδίου εφαρμογής όλοι οι ψηφιοποιημένοι τομείς της εσωτερικής αγοράς της Ένωσης.[274] Αυτό έχει ως συνέπεια, να εκτίθενται σε εγγενείς κινδύνους σημαντικοί τομείς οι οποίοι παραμένουν αρρύθμιστοι, διακυβεύοντας την εύρυθμη λειτουργία της εσωτερικής αγοράς.[275] Η δεύτερη αδυναμία του ρυθμιστικού

[271] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[272] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[273] Ibid *supra* 77, pp. 226-235.

[274] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[275] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

πλαισίου της οδηγίας συνίσταται στην ασάφεια κατά τον προσδιορισμό της έννοιας των φορέων εκμετάλλευσης βασικών υπηρεσιών και παρόχων ψηφιακών υπηρεσιών.[276] Αυτή η ασάφεια υπονομεύει την ομοιόμορφη εφαρμογή των διατάξεων της οδηγίας από τα κράτη μέλη, ιδίως εάν ληφθεί υπόψη ότι ορισμένα είδη οντοτήτων δεν έχουν προσδιοριστεί καθολικά σε όλα τα κράτη μέλη με τον ίδιο τρόπο.[277] Προς τούτο, η Επιτροπή αναφέρει ως παράδειγμα ότι «*ορισμένα μεγάλα νοσοκομεία σε ένα κράτος μέλος δεν εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS και, ως εκ τούτου, δεν υποχρεούνται να εφαρμόζουν τα ανάλογα μέτρα ασφάλειας, ενώ σε άλλο κράτος μέλος σχεδόν όλοι οι πάροχοι υγειονομικής περίθαλψης στη χώρα καλύπτονται από τις απαιτήσεις ασφάλειας της οδηγίας NIS*».[278]

Τρίτον, η οδηγία παρέχει σύμφωνα με την Επιτροπή ιδιαίτερα ευρεία διακριτική ευχέρεια στα κράτη μέλη ως προς τις απαιτήσεις ασφάλειας και κοινοποίησης των αναφορών απειλής.[279] Η ευρεία αυτή διακριτική ευχέρεια των κρατών μελών μπορεί να καταστήσει αναποτελεσματική την εφαρμογή των κανόνων της οδηγίας και κατ' επέκταση να έχει δυσμενείς συνέπειες για την ανθεκτικότητα του κυβερνοχώρου.[280] Τέλος, εκτιμάται ότι τα κράτη μέλη είναι απρόθυμα να επιβάλλουν κυρώσεις για παραβιάσεις των κανόνων που υιοθετήθηκαν αναφορικά με τις απαιτήσεις για ασφάλεια και αναφοράς περιστατικών στις αρμόδιες αρχές.[281] Η ευελιξία και το εύρος της διακριτικής ευχέρειας που παρέχει σε αυτά η υφιστάμενη οδηγία φαίνεται να επιτρέπει αυτήν την επιζήμια αδράνεια. Τέλος, η έλλειψη στενής

[276] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[277] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[278] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[279] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[280] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[281] Ibis *supra* 22 (Βλ. Αιτιολογική Έκθεση).

συνεργασίας για ανταλλαγή πληροφορίων μεταξύ των κρατών μελών δυσχεραίνει την αποτελεσματικότητα των μέτρων για υποστήριξη και ενδυνάμωση του κυβερνοχώρου.[282]

Επιπλέον, αξίζει να σημειωθεί ότι η Επιτροπή στην πρόταση της για αναθεώρηση της οδηγίας, αποτυπώνει στο κείμενο της την έννοια της κυβερνοασφάλειας. Η έννοια της κυβερνοασφάλειας στην υπάρχουσα οδηγία δεν εντοπίζεται.[283] Ενώ στην ανακοίνωση που εξέδωσε το 2013 η Επιτροπή και ο Ύπατος Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας, αναφέρθηκε η ανάγκη για ρύθμιση του κυβερνόχωρου.[284] Εν συνεχεία στη νομοθετική πρωτοβουλία της Επιτροπής για τη θέσπιση της Οδηγίας NIS η εν λόγω έννοια απουσίαζε από το τελικό κείμενο της.[285] Η απουσία της ανωτέρω έννοιας ενδεχομένως να οδήγησε στη μη δημιουργία της απαιτούμενης «κουλτούρας και νοοτροπίας» από τα κράτη μέλη για τη διαφύλαξη του κυβερνοχώρου μεσώ των δικών τους ενεργειών.[286] Στην προκειμένη περίπτωση, η Επιτροπή πλέον κάνει ειδική αναφορά. Ειδικότερα, το άρθρο 4 παράγραφος 3 του της πρότασης, ως προς τον ορισμό της κυβερνοασφάλειας παραπέμπει στον *Κανονισμού (ΕΕ) 2019/881(25).*[287] Σύμφωνα με τον Κανονισμό (ΕΕ)2019/881 η κυβερνοασφάλεια ορίζεται ως οι «*δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και*

[282] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[283] Ibid *supra* 77, pp. 223-224.

[284] Ibid *supra* 77, pp. 223-224.

[285] Ibid *supra* 77, pp. 223-224.

[286] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[287] Ibid *supra supra* 22, Άρθρο 4 της Πρότασης.

πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων».[288]

Περαιτέρω, στο κείμενο της πρόταση συμπεριλαμβάνεται και η έννοια της κυβερνοαπειλής, η οποία σύμφωνα με την παράγραφο 7 του άρθρου 4 της πρότασης, έχει τον ίδιο ορισμό με αυτό που δίδεται στον Κανονισμός (ΕΕ)2019/881.[289] Ο εν λόγω κανονισμός προβλέπει ότι ως κυβερνοαπειλή κρίνεται «*κάθε πιθανή περίσταση, πιθανό συμβάν ή πιθανή ενέργεια που θα μπορούσε να καταστρέψει, να διαταράξει ή να επιδράσει κατ' άλλον τρόπο δυσμενώς στα συστήματα δικτύου και πληροφοριών, στους χρήστες των εν λόγω συστημάτων και σε άλλα πρόσωπα».*[290] Με την αποτύπωση των ως άνω εννοιών στην αναθεωρημένη οδηγία, γίνεται πλέον ξεκάθαρα αντιληπτό ότι πρωταρχικός σκοπός του εν λόγω ρυθμιστικού πλαισίου είναι η διασφάλιση της ανθεκτικότητας του κυβερνόχωρου μέσω των απαιτήσεων κυβερνοασφάλειας που οφείλουν να διασφαλίζουν όλα τα κράτη μέλη. Κατ' επέκταση μέσω των ανωτέρω απαιτήσεων αντιμετωπίζεται και κάθε κυβερνοαπειλή που ενδεχομένως να οδηγούσε στον κλονισμό της εύρυθμης λειτουργίας της εσωτερικής αγοράς της Ένωσης.

(Α) Επέκταση πεδίου εφαρμογής

Στην πρόταση, η Επιτροπή λαμβάνοντας υπόψη τις πρακτικές αστοχίες και τους περιορισμούς που θέτει η Οδηγίας NIS στο πεδίο εφαρμογής της, προτείνει την διεύρυνσή της. Η πρόταση καταργεί την διάκριση των οντοτήτων σε φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών λόγω της

[288] Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια). https://eur-lex.europa.eu/legal-content/el/ALL/?uri=CELEX:32019R0881

[289] Ibid *supra* 22, Άρθρο 4 της Πρότασης.

[290] Ibid *supra* 288.

ασάφειας των εννοιών αυτών.[291] Ως εκ τούτου σύμφωνα με το άρθρο 2 παράγραφος 1 της πρότασης, οι οντότητες που θα εμπίπτουν πλέον στο πεδίο εφαρμογής της αναθεωρημένης οδηγίας είναι αυτές που κατηγοριοποιούνται σε βασικές και σημαντικές οντότητες.[292] Σύμφωνα με το άρθρο 4 της πρότασης, οι οντότητες που κρίνονται ως βασικές είναι αυτές που εμπίπτουν στο Παράρτημα Ι. Σύμφωνα με το Παράρτημα Ι, ως βασικές οντότητες θεωρούνται οι δημόσιες ή ιδιωτικές οντότητες που δραστηριοποιούνται στην ενέργεια, στις μεταφορές, στις τράπεζες, στις υποδομές χρηματοπιστωτικών αγορών, στην υγεία, στο πόσιμο νερό, στα λύματα, στις ψηφιακές υποδομές, στη δημόσια διοίκηση και στο διάστημα.[293] Παράλληλα, οι οντότητες που καθορίζονται ως σημαντικές είναι αυτές που εμπίπτουν στο Παράρτημα ΙΙ.[294] Σύμφωνα με το Παράρτημα ΙΙ ως σημαντικές θεωρούνται οι ιδιωτικές ή δημόσιες οντότητες που εμπίπτουν στις ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών, στη διαχείριση αποβλήτων, στην παραγωγή και διανομή χρημάτων, στον κατασκευαστικό τομέα και στους ψηφιακούς παρόχους.[295]

Εν πρώτοις, παρατηρείται ότι η Επιτροπή επιχειρεί λόγω της ασάφειας της έννοιας των φορέων εκμετάλλευσης βασικών υπηρεσιών και παρόχων ψηφιακών υπηρεσιών, να διαφοροποιήσει την ονομασία των οντοτήτων που θα εμπίπτουν στο πεδίο εφαρμογής της αναθεωρημένης οδηγίας. Αυτό γίνεται χωρίς όμως στο κείμενο της πρότασης να επεξηγούνται περαιτέρω οι έννοιες «βασικές και σημαντικές». Ωστόσο, ενδεχομένως και να μην χρειάζεται οποιαδήποτε περαιτέρω επεξήγηση των ανωτέρων εννοιών, καθότι οι ανωτέρω έννοιες συσχετίζονται με τον ρόλο που

[291] Ildiko Angeli, Eszter Sieber-Fazakas, «Automotive Sector Within the Scope of Planned NIS II Cybersecurity Rules», Budapest Business Journal, 2021, Vol. 29, Issue 10, p13.

[292] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[293] Ibid *supra* 22, Παράρτημα Ι της Πρότασης.

[294] Ibid *supra* 22, Παράρτημα Ι της Πρότασης.

[295] Ibid *supra* 22, Παράρτημα ΙΙ της Πρότασης.

διαδραματίζουν στην εσωτερική αγορά της Ένωσης.[296] Ως βασικές οντότητες ενδεχομένως να κρίνονται αυτές που είναι βασικές για την ίδια τη λειτουργία της εσωτερικής αγοράς και ως εκ τούτου, σε περίπτωση ενδεχόμενης διατάραξης τους να οδηγήσουν σε αποδιοργάνωση της εσωτερικής αγοράς. Ενώ, οι σημαντικές οντότητες είναι αυτές που αφενός δεν έχουν την ίδια βαρύτητα με τις βασικές οντότητες, όμως σε περίπτωση διατάραξης τους πάλι θα επηρεαστεί σημαντικά η εύρυθμη λειτουργία της εσωτερικής αγοράς της Ένωσης. Συνεπώς, θα μπορούσε να θεωρηθεί ότι οι βασικές οντότητες επηρεάζουν την ίδια την λειτουργία της εσωτερικής αγοράς και οι σημαντικές οντότητες την εύρυθμη λειτουργία της εσωτερικής αγοράς. Επιπλέον, σύμφωνα με το άρθρο 4 της πρότασης, η έννοια οντότητα διευρύνεται περιλαμβάνοντας *«κάθε φυσικό ή νομικό πρόσωπο που έχει συσταθεί και αναγνωρίζεται ως τέτοιο σύμφωνα με το εθνικό δίκαιο του τόπου εγκατάστασής του, το οποίο μπορεί, ενεργώντας εξ ιδίου ονόματος, να ασκεί δικαιώματα και να αναλαμβάνει υποχρεώσεις»*.[297]

Η αλλαγή βέβαια της ονομασίας των κατηγοριών, στις οποίες εμπίπτουν οι οντότητες, επί της ουσίας, μπορεί να αναφέρει κανείς ότι δεν θα επιφέρει κάποια σημαντική διαφοροποίηση συγκριτικά με την υπάρχουσα οδηγία. Εφόσον οι υφιστάμενοι φορείς εκμετάλλευσης βασικών υπηρεσιών θα μετονομαστούν σε βασικές οντότητες και οι πάροχοι ψηφιακών υπηρεσιών σε σημαντικές οντότητες. Ενδέχεται και πάλι η κατηγοριοποίηση σε βασικές και σημαντικές να μην είναι εύκολη διαδικασία.[298] Ωστόσο, στο κομμάτι αυτό παρατηρούνται δύο αλλαγές. Πρώτον, η διεύρυνση σημαντικά του πεδίου εφαρμογής με την ένταξη νέων

[296] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[297] Ibid *supra* 22, Άρθρο 4 της Πρότασης.

[298] Thomas Siever «Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations», International Cybersecurity Law Review, 2021, pp. 224-225.

τομέων/υποτομέων και η προσθήκη των φυσικών προσώπων στην έννοια της οντότητας.[299] Δεύτερον, η εισαγωγή ενός ενιαίου κριτήριου προσδιορισμού, το οποίο θα κρίνει κατά πόσο οι εν λόγω οντότητες εμπίπτουν ή όχι στο πεδίο εφαρμογής της αναθεωρημένης οδηγίας.[300] Κατ' αρχάς, παρατηρείται από τα Παραρτήματα της πρότασης μια σημαντική επέκταση του πεδίου εφαρμογής. Στο Παράρτημα Ι, οι τομείς που θα εμπίπτουν στο πεδίο εφαρμογής έχουν αυξηθεί από επτά στους δέκα και στο Παράρτημα ΙΙ έχουν ενταχθεί επιπρόσθετοι πέντε νέοι τομείς.[301]

Ειδικότερα, στο Παράρτημα Ι έχουν ενταχθεί οι ψηφιακές υποδομές, η δημόσια διοίκηση και το διάστημα.[302] Οι δύο από τους τρείς νέους τομείς εντάχθηκαν στο Παράρτημα Ι ενδεχομένως λόγω της διαφορετικής υφιστάμενης πρακτικής που ακολουθούν τα κράτη μέλη. Η Ισπανία για παράδειγμα πέραν από τους επτά τομείς που καθόριζε η τρέχουσα οδηγία, ενσωμάτωσε στο εσωτερικό της τη δημόσια διοίκηση και το διάστημα.[303] Το ίδιο έκανε και η Κύπρος με την ένταξη της δημόσιας διοίκησης.[304] Οι τομείς όμως αυτοί δεν έχουν ενσωματωθεί από όλα τα κράτη μέλη. Με συνέπεια να παρατηρείται μια σημαντική ανομοιομορφία ως προς τις οντότητες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS.[305] Για την εμπόδιση του κατακερματισμού, η πρόταση προτείνει την καθολική εναρμόνιση των κρατών μελών μέσω της ένταξης των δύο αυτών τομέων. Περαιτέρω, η πρόταση εισηγείται την ενσωμάτωση και των κρίσιμων υποδομών αφενός λόγω της μεγάλης αλληλεξάρτησης

[299] Ibid 298, pp. 224-225

[300] Ibid *supra* 298, pp. 224-225.

[301] Ibid *supra* 22, Παράρτημα Ι και ΙΙ της Πρότασης.

[302] Ibid *supra* 22, Παράρτημα ΙΙ της Πρότασης.

[303] Ibid *supra* 108.

[304] Ibid *supra* 108.

[305] Ibid *supra* 108.

τους με την οικονομία της ένωσης.[306] Το ίδιο αφετέρου ισχύει και με τους νέους τομείς του ενσωματώθηκαν στο Παράρτημα ΙΙ, όπως οι ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών, η διαχείριση αποβλήτων, η παραγωγή και διανομή χρημάτων και ο κατασκευαστικό τομέα. Κατ' επέκταση, η επιθυμία της Επιτροπής για σημαντική διεύρυνση του πεδίου εφαρμοφής, καλύπτοντας περισσότερους τομείς και υποτομείς, έγκειται όπως φαίνεται και στην αιτιολογική σκέψη αφενός στην αυξημένη ψηφιοποίηση και αφετέρου στην διαφορετική πρακτική μεταξύ των κρατών μελών.[307] Συνεπώς, οι στόχοι που θέτει η Επιτροπή στην αιτιολογική σκέψη της πρότασης φαίνεται να επιδιώκονται πιο αποτελεσματικά μέσα από τις διατάξεις της νέας αναθεωρημένης οδηγίας.

Περαιτέρω, το άρθρο 2 της πρότασης θέτει ένα επιπρόσθετο κριτήριο για όλες τις οντότητες που εντάσσονται στο Παράρτημα Ι και Παράρτημα ΙΙ. Το κριτήριο αυτό θα είναι ενιαίο και θα πρέπει όλες οι οντότητες να το πληρούν για να θεωρηθούν ότι εμπίπτουν στο πεδίο εφαρμογής της αναθεωρημένης οδηγίας. Επομένως, δεν εμπίπτουν «αυτόματα» όλες οι οντότητες που υπάρχουν στα Παραρτήματα της πρότασης στο πεδίο εφαρμογής της αναθεωρημένης οδηγίας.[308] Ειδικότερα, σύμφωνα με το άρθρο 2 παράγραφος 1 της πρότασης, η *«παρούσα οδηγία δεν εφαρμόζεται σε οντότητες που χαρακτηρίζονται ως πολύ μικρές και μικρές επιχειρήσεις κατά την έννοια της σύστασης 2003/361/ΕΚ της Επιτροπής».*[309] Σύμφωνα με άρθρο 2 παράγραφος 2 της σύστασης 2003/361/ΕΚ της Επιτροπής, ως μικρή επιχείρηση θεωρείται *«η επιχείρηση που απασχολεί λιγότερους από 50 εργαζομένους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 10*

[306] Ibis *supra* 22, (Βλ. Αιτιολογική Έκθεση).

[307] Ibid *supra* 298, pp. 224-225.

[308] Ibid *supra* 298, pp. 224-225.

[309] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

εκατομμύρια ευρώ» και ως πολύ μικρή *αυτή «η οποία απασχολεί λιγότερους από δέκα εργαζομένους και της οποίας ο ετήσιος κύκλος εργασιών ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 2 εκατομμύρια ευρώ».*[310] Κατά συνέπεια, οι οντότητες που θεωρούνται «*πολύ μικρές*» ή «*μικρές*» κατά την ανωτέρω σύσταση της Επιτροπής, ακόμη και εάν εντάσσονται στα Παραρτήματα της αναθεωρημένη οδηγίας, αποκλείονται από το πεδίο εφαρμογής της[311].

Ενώ η υπάρχουσα οδηγία προβλέπει ότι τα κράτη μέλη είναι υπεύθυνα για να προσδιορίσουν, δυνάμει του άρθρου 5, τις οντότητες που εμπίπτουν στους φορείς εκμετάλλευσης βασικών υπηρεσιών, η πρόταση πλέον δεν παρέχει μια τέτοια πρόβλεψη.[312] Στην αιτιολογική σκέψη της πρότασης, η Επιτροπή αναφέρει ότι κατά τον προσδιορισμό των οντοτήτων, οι «*οικονομικοί και ανθρώπινοι πόροι που διαθέτουν τα κράτη μέλη για την εκπλήρωση των καθηκόντων τους*» οδήγησαν «*σε διαφορετικά επίπεδα ωριμότητας στην αντιμετώπιση των κινδύνων κυβερνοασφάλειας».*[313] Επιπλέον, κατά την εναρμόνιση της οδηγίας NIS τα κράτη μέλη έπρεπε πρώτα να προσδιορίσουν τους φορείς εκμετάλλευσης βασικών υπηρεσιών.[314] Το γεγονός αυτό οδήγησε στην καθυστέρηση της άμεσης και αποτελεσματικής εφαρμογής της οδηγίας NIS, η οποία εντέλει τέθηκε σε εφαρμογή από τις 9 Νοεμβρίου 2018.[315] Η καθυστέρηση των έξι μηνών άφησε τόσο τα κράτη μέλη της Ένωσης όσο και την εσωτερική αγορά εκτεθειμένα σε κινδύνους και

[310] Ibid *supra* 133.

[311] Christoph Haid, Felix Schneider «Cybersecurity on the rise: The NIS Directive 2.0», Schonherr, Πρόσβαση 15/11/2021. https://www.schoenherr.eu/content/cybersecurity-on-the-rise-the-nis-directive-2-0/

[312] Ibis *supra* 298, pp. 225-226.

[313] Ibid *supra* 22 (Βλ. Αιτιολογική Έκθεση).

[314] Ibid *supra* 298, pp. 225-226.

[315] Ibid *supra* 298, pp. 225-226.

απειλές. Γι' αυτό πλέον και η Επιτροπή κρίνει ότι ίδιο το *«μέγεθος»* της κάθε οντότητας πρέπει να είναι καθοριστικό για το αν εμπίπτει ή όχι στο πεδίο εφαρμογής της πρότασης.[316] Εντούτοις, η πρόταση περιέχει μια επιφύλαξη σχετικά με τις οντότητες που εξαιρούνται λόγω «μεγέθους».[317] Σύμφωνα με το άρθρο 2 παράγραφος 2 της πρότασης ανεξάρτητα από το μέγεθος μια οντότητας μπορεί αυτή να εφαρμόζει την οδηγία εάν εμπίπτει στις περιπτώσεις που αναφέρονται κατωτέρω. [318]

Η πρώτη περίπτωση που σύμφωνα με το εδάφιο α' εμπίπτει στην επιφύλαξη, είναι οντότητες των οποίων *«οι υπηρεσίες» είτε* αφορούν *«δημόσια δίκτυα ηλεκτρονικών επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών που αναφέρονται στο παράρτημα I σημείο 8»,* είτε αφορούν *«παρόχους υπηρεσιών εμπιστοσύνης που αναφέρονται στο παράρτημα I σημείο 8»* και τέλος εάν αφορούν *«μητρώα ονομάτων τομέα ανωτάτου επιπέδου και παρόχου υπηρεσιών του συστήματος ονομάτων τομέα (DNS) που αναφέρονται στο παράρτημα I σημείο 8».*[319] Η δεύτερη περίπτωση σύμφωνα με το εδάφιο β' αφορά οντότητες που είναι φορείς «*δημόσιας διοίκησης όπως ορίζεται στο άρθρο 4 σημείο 23».*[320] Η τρίτη περίπτωση σύμφωνα με το εδάφιο γ' εάν πρόκειται για *«οντότητα είναι ο μοναδικός πάροχος υπηρεσίας σε κράτος μέλος».*[321] Η τέταρτη, σύμφωνα με το εδάφιο δ΄ αφορά οντότητες, οι οποίες *«σε ενδεχόμενη διατάραξη της υπηρεσίας»* που παρέχουν «*θα μπορούσε να έχει επιπτώσεις στη δημόσια ασφάλεια, στη δημόσια προστασία ή στη*

[316] Ibid *supra* 298, pp. 225-226.

[317] Ibid *supra* 298, pp. 225-226.

[318] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[319] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[320] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[321] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

δημόσια υγεία».[322] Η πέμπτη περίπτωση, σύμφωνα με το εδάφιο ε', αφορά οντότητες, η ενδεχομένη διατάραξη των οποίων *«θα μπορούσε να προκαλέσει συστημικούς κινδύνους, ιδίως για τους τομείς στους οποίους η διαταραχή αυτή θα μπορούσε να έχει διασυνοριακό αντίκτυπο»*.[323] Η έκτη περίπτωση σύμφωνα με το εδάφιο στ', αφορά οντότητες, οι οποίες θεωρούνται ως κρίσιμες *«λόγω της ιδιαίτερης σημασίας τους σε περιφερειακό ή εθνικό επίπεδο για τον συγκεκριμένο τομέα ή είδος υπηρεσίας ή για άλλους αλληλοεξαρτώμενους τομείς στο κράτος μέλος»*.[324] Τέλος, σύμφωνα με το εδάφιο ζ', οι οντότητες που χαρακτηρίζεται ως κρίσιμες «*σύμφωνα με την οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων* » ή *ως* ισοδύναμες «*με κρίσιμη οντότητα, σύμφωνα με το άρθρο 7 της εν λόγω οδηγίας»*.[325]

Σύμφωνα το άρθρο 2 παράγραφος 2 της πρότασης τα κράτη μέλη είναι υπεύθυνα για τις οντότητες που εντάσσονται στις επιφυλάξεις των εξαιρέσεων και γι' αυτό θα πρέπει να καταρτίσουν κατάλογο των οντοτήτων αυτών (εκτός της πρώτης περίπτωσης) και να τον υποβάλλουν στην Επιτροπή εντός έξι μηνών μετά την προθεσμία ενσωμάτωσης της οδηγίας στην εσωτερική έννομη τάξη τους.[326] Ο κατάλογος αυτός θα πρέπει ανά διετία να επαναξιολογείται και όπου κρίνεται αναγκαίο να επικαιροποιείται.[327] Η επιφύλαξη των εξαιρέσεων, επεκτείνει περαιτέρω το πεδίο εφαρμογή της οδηγίας οδηγώντας σε μια σημαντική αύξηση των οντοτήτων που καλύπτονται από το πεδίο εφαρμογής της πρότασης. Η αύξηση των αριθμών των

[322] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[323] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[324] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[325] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[326] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

[327] Ibid *supra* 22, Άρθρο 2 της Πρότασης.

οντοτήτων που θα καλύπτεται υπολογίζεται να είναι επταπλάσια.[328] Με αυτόν τον τρόπο η Επιτροπή προσπαθεί να βελτιώσει την ανθεκτικότητα σε όλους σχεδόν τους τομείς που επηρεάζουν είτε έμμεσα είτε άμεσα την εσωτερική αγορά της Ένωσης.[329]

(Β) Κοινές Απαιτήσεις Ασφάλειας και Αναφοράς Περιστατικών

Περαιτέρω, η Επιτροπή προτείνει τόσο οι βασικές οντότητες όσο και οι σημαντικές οντότητες, να υπόκεινται από κοινού στις ίδιες απαιτήσεις ασφάλειας.[330] Ειδικότερα, το άρθρο 18 της πρότασης αναφέρει ότι *οι βασικές και σημαντικές οντότητες θα πρέπει να «λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια δικτυακών και πληροφοριακών συστημάτων που χρησιμοποιούν οι εν λόγω οντότητες κατά την παροχή των υπηρεσιών τους».*[331] Ως προς τα μέτρα ασφάλειας, συμπληρώνει το άρθρο 18, παράγραφος 1 αναφέροντας ότι θα πρέπει να λαμβάνονται υπόψη και οι *«πλέον πρόσφατες τεχνικές δυνατότητες […]ανάλογα προς τον εκάστοτε κίνδυνο».*[332] Η αναφορά στις πρόσφατες τεχνικές δυνατότητες απαιτεί μια συνεχή ενημέρωση και εγρήγορση των οντοτήτων ως προς τις τεχνολογικές εξελίξεις για την αντιμετώπιση των κινδύνων με προσαρμοσμένες και καινοτόμες απαντήσεις (ως αναφέρει η Επιτροπή στην πρότασή της).[333] Η απαίτηση βέβαια για *«αναλογικά τεχνικά και οργανωτικά μέτρα»* δεν διαφοροποιείται σημαντικά από τα άρθρα 14 και 16 της Οδηγίας NIS, εφόσον παραμένει η ίδια.[334] Ούτε στο κείμενο της πρότασης

[328] Ibid *supra* 298, pp. 225-227.

[329] Ibid *supra* 298, pp. 225-227.

[330] Ibid *supra* 298, pp. 223.

[331] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

[332] Ibid supra 22, Άρθρο 18 της Πρότασης.

[333] Ibid supra 22, Άρθρο 18 της Πρότασης.

[334] Ibid *supra* 298, pp. 223.

επεξηγούνται οι εν λόγω έννοιες περαιτέρω. Ιδιαίτερο, ενδιαφέρον ως προς αυτό, παρουσιάζει το άρθρο 18 παράγραφος 2, η οποία αναφέρεται στα μέτρα που θα πρέπει να ληφθούν «*τουλάχιστον»* υπόψη.[335] Με αποτέλεσμα, μέσω της εν λόγω παραγράφου να επιχειρείται ένας κατ' ελάχιστο προσδιορισμός των μέτρων που θα πρέπει να λάβουν όλες οι οντότητες των κρατών μελών που εμπίπτουν στο πεδίο εφαρμογής της αναθεωρημένης πρότασης.[336]

Το πρώτο μέτρο σύμφωνα με το εδάφιο α' αφορά τις *«πολιτικές αναλύσεις κινδύνων και ασφάλεια του πληροφοριακού συστήματος».*[337] Το δεύτερο μέτρο σύμφωνα με το εδάφιο β' αφορά *«στον χειρισμό των περιστατικών»* και ειδικότερα μέσω *«της πρόληψης, ανίχνευσης και αντιμετώπισης των περιστατικών».*[338] Το τρίτο μέτρο, σύμφωνα με το εδάφιο γ', αφορά στη *«συνέχιση των δραστηριοτήτων και διαχείριση των κρίσεων».*[339] Εν προκειμένω, προφανώς και η Επιτροπή απαιτεί από τις οντότητες ότι ακόμη και σε ενδεχόμενο διατάραξης, οι οντότητες θα καταβάλλουν την ύστατη προσπάθεια για συνέχιση των υπηρεσιών τους με την παράλληλη αντιμετώπιση των κινδύνων που βρίσκονται υπό εξέλιξη. Το τέταρτο μέτρο, σύμφωνα με το εδάφιο δ, αφορά στην *«ασφάλεια της αλυσίδας εφοδιασμού συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ της κάθε οντότητας και των προμηθευτών της ή των παρόχων υπηρεσιών, όπως οι πάροχοι υπηρεσιών αποθήκευσης και επεξεργασίας δεδομένων ή υπηρεσιών διαχείρισης ασφάλειας».*[340] Το πέμπτο μέτρο, σύμφωνα με το εδάφιο ε' την ασφάλεια

[335] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

[336] Ibid *supra* 298, pp. 228-229.

[337] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

[338] Ibid *supra* 22, Άρθρο 18 της Πρότασης

[339] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

[340] Ibid *supra* 22, Άρθρο 18 της Πρότασης

κατά την *«απόκτηση, ανάπτυξη και συντήρηση δικτυακών και πληροφοριακών συστημάτων, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης τρωτών σημείων»*.[341] Το έκτο μέτρο, σύμφωνα με το εδάφιο στ', αφορά στις *«πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας»*, ιδίως μέσω *«δοκιμών και ελέγχων»*.[342] Τέλος σύμφωνα με το εδάφιο ζ', απαιτείται οι οντότητες να χρησιμοποιούν *«την κρυπτογράφηση και τη κρυπτοθέτηση»*.[343] Από τα προαναφερθέντα μέτρα που επιβάλλει σωρευτικά και καθολικά η Επιτροπή, γίνεται αντιληπτό ότι γίνεται μια προσπάθεια λήψης τόσο προληπτικών όσο και κατασταλτικών μέτρων με σκοπό τη διαχείριση ενδεχόμενων κινδύνων.[344] Η τρέχουσα οδηγία δεν προσδιορίζει στα άρθρα 14 και 16 καθόλου ποια μέτρα οφείλουν να λαμβάνουν οι οντότητες. Εν προκειμένω, με τον προσδιορισμό των ελάχιστων μέτρων διασφαλίζεται αφενός ένα συγκεκριμένο επίπεδο ωριμότητας των κρατών μελών και αφετέρου μια ομοιομορφία στον τρόπο αντιμετώπισης των κινδύνων σε ολόκληρη την Ένωση.[345]

Η Επιτροπή επιπρόσθετα, απαιτεί κατά το άρθρο 18, παράγραφος 3 από τα κράτη μέλη να ελέγχουν ότι οι οντότητες που βρίσκονται στην επικράτεια τους τηρούν τα ανωτέρω μέτρα.[346] Γι' αυτό και απαιτεί σε περίπτωση που μια οντότητα δεν λαμβάνει υπόψη τα εν λόγω μέτρα *«χωρίς αδικαιολόγητη καθυστέρηση»* να φροντίσει (ίσως μέσω συγκεκριμένων μηχανισμών) να ληφθούν τα *«αναγκαία διορθωτικά μέτρα»* για να διασφαλιστεί η συμμόρφωση τους. Εναπόκειται κατά την

[341] Ibid *supra* 22, Άρθρο 18 της Πρότασης

[342] Ibid *supra* 22, Άρθρο 18 της Πρότασης

[343] Ibid *supra* 22, Άρθρο 18 της Πρότασης

[344] Ibid *supra* 298, pp. 229-230.

[345] Ibid *supra* 298, pp. 229-230.

[346] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

ενσωμάτωση της να δούμε ποια μέτρα θα επιλέξουν τα κράτη μέλη να υιοθετήσουν.[347]Ενδεχομένως, να επιβάλλουν κυρώσεις ως προς τη μη συμμόρφωση τους με τις de minimum απαιτήσεις ασφάλειας. Επιπλέον, ως προς το ζήτημα των μέτρων η πρόταση αναφέρει ότι η Επιτροπή «*μπορεί και να εκδίδει εκτελεστικές πράξεις για τον καθορισμό των τεχνικών και μεθοδολογικών προδιαγραφών*» των εν λόγω μέτρων.[348] Συνεπώς, θα υπάρχουν καθοδηγητικές οδηγίες για το πως θα πρέπει να ενεργούν.

Ωστόσο, το άρθρο 18, παράγραφος 6 παρουσιάζει το μεγαλύτερο ενδιαφέρον. Σύμφωνα λοιπόν με αυτό *«η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις, σύμφωνα με το άρθρο 36, για συμπλήρωση των στοιχείων που ορίζονται στην παράγραφο 2, ώστε να λαμβάνονται υπόψη νέες κυβερνοαπειλές, τεχνολογικές εξελίξεις ή τομεακές ιδιαιτερότητές».[349]* Επί της ουσίας, η διάταξη αυτή αναφέρει ότι η Επιτροπή μπορεί να τροποποιεί τα μέτρα χωρίς να χρήζει αναθεώρησης η ίδια η Οδηγία. Η ευχέρεια αυτή που παρέχεται φαίνεται να είναι απολύτως αναλογική ενόψει των αυξανόμενων απειλών, οι οποίες μετεξελίσσονται συνεχώς και εφόσον σύμφωνα με το άρθρο 36 αφορά για συγκεκριμένη χρονική περίοδο. Στόχος της Επιτροπής είναι τα μέτρα ασφάλειας να είναι συνεχώς προσαρμοσμένα στις τεχνολογικές εξελίξεις και καινοτόμα για την ουσιαστική αντιμετώπιση των ενδεχόμενων κινδύνων και απειλών.

Επιπλέον, μέσω της εν λόγω διάταξης δίνεται και η απάντηση σε όσους κρίνουν ότι το ορθότερο νομοθετικό μέσο για την αντιμετώπιση των εν λόγω ζητημάτων είναι η θέσπιση σχετικού κανονισμού. Για παράδειγμα η Επιτροπή για την

[347] Ibid *supra* 298, pp. 229-230.

[348] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

[349] Ibid *supra* 22, Άρθρο 18 της Πρότασης.

προστασία των προσωπικών δεδομένων αποφάσισε να υιοθετήσει τον Κανονισμό GDPR για το άμεσο αποτέλεσμα της ρύθμισής της. Εν προκειμένω, μπορεί η υπάρχουσα οδηγία να έχει παρουσιάσει στο προσκήνιο σχετικές αδυναμίες, εντούτοις η Επιτροπή αναφέρει στην αιτιολογική της σκέψη ότι το μέσο αντιμετώπισης των εν λόγω ζητημάτων θα γίνει μέσω μιας νέας οδηγίας, καθότι στόχος είναι *«να παρασχεθεί στα κράτη μέλη η απαιτούμενη ευελιξία ώστε να ληφθούν υπόψη οι εθνικές ιδιαιτερότητες».*[350] Επομένως, θα μπορεί κάνεις να αναφέρει ότι η ευελιξία αυτή που δόθηκε με την τρέχουσα οδηγία στα κράτη μέλη, είναι αυτή που οδήγησε και στην αναποτελεσματικότητα της εφαρμογής της. Συνεπώς γιατί να επιλεγεί πάλι ως ρυθμιστικό μέσο την οδηγία; Εν προκειμένω, η Επιτροπή στην αναθεωρημένη πρόταση της προσθέτει αρκετές δικλείδες ασφαλείας για την αποτελεσματικότητα της ρύθμισης της και μια εξ αυτών είναι και η διάταξη της παραγράφου 6 του άρθρου 18.

Επιπροσθέτως, προκειμένου να αποδειχθεί η συμμόρφωση εκ μέρους των βασικών και σημαντικών οντοτήτων με ορισμένες από τις απαιτήσεις που καθορίζονται στο άρθρο 18, προβλέπεται ότι τα κράτη μέλη μπορούν δυνάμει του άρθρου 21 «*να απαιτήσουν από τις βασικές και σημαντικές οντότητες να πιστοποιούνται ορισμένα προϊόντα ΤΠΕ, υπηρεσίες ΤΠΕ και διαδικασίες ΤΠΕ στο πλαίσιο συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας που εγκρίνονται σύμφωνα με το άρθρο 49 του Κανονισμού (ΕΕ) 2019/881*».[351] Στην παράγραφο 2 του εν λόγω άρθρου διευκρινίζεται ότι «*θα προσδιορίζονται από ποιες κατηγορίες βασικών οντοτήτων θα απαιτείται η λήψη πιστοποιητικού και δυνάμει ποιων συγκεκριμένων ευρωπαϊκών συστημάτων πιστοποίησης κυβερνοασφάλειας*».[352]

[350] Ibid *supra* 22, (Βλ. Αιτιολογική Έκθεση).

[351] Ibid *supra* 22, (Βλ. Αιτιολογική Έκθεση).

[352] Ibid *supra* 22, Άρθρο 21 της Πρότασης

Με την παράγραφο αυτή, η Επιτροπή επιχειρεί μέσω ασφαλιστικών δικλείδων να θέσει πλαίσια στην ευθύνη και λογοδοσία των οντοτήτων κατά τη συμμόρφωση τους με τις απαιτήσεις για ασφάλεια στον κυβερνόχωρο.[353]

Πέραν από τα κοινά μέτρα διαχείρισης κινδύνων, η Επιτροπή προτείνει και κοινές υποχρεώσεις για αναφορά περιστατικών και από τις δύο οντότητες.[354] Σύμφωνα με το άρθρο 20 παράγραφος 1 «*οι βασικές και σημαντικές οντότητες κοινοποιούν, χωρίς αδικαιολόγητη καθυστέρηση, στις αρμόδιες αρχές ή στην CSIRT, σύμφωνα με τις παραγράφους 3 και , κάθε περιστατικό που έχει σημαντικό αντίκτυπο στην παροχή των υπηρεσιών τους».*[355] Σύμφωνα με την διάταξη της παραγράφου 3 ένα περιστατικό θεωρείται ως σημαντικό εάν «*προκάλεσε ή έχει τη δυνατότητα να προκαλέσει σημαντική λειτουργική διαταραχή ή οικονομικές ζημίες στην οικεία οντότητά»* ή εάν «*έχει επηρεάσει ή έχει τη δυνατότητα να επηρεάσει άλλα φυσικά ή νομικά πρόσωπα προκαλώντας σημαντικές υλικές ή μη υλικές ζημίες*».[356] Η παράγραφος 4 του εν λόγω άρθρου καθορίζει ένα λεπτομερές και κλιμακωτό σχέδιο δράσης των οντοτήτων. Σύμφωνα με το εδάφιο α' οι οντότητες θα πρέπει κατ' αρχή *«χωρίς αδικαιολόγητη καθυστέρηση και σε κάθε περίπτωση εντός 24 ωρών από τη στιγμή που έλαβαν γνώση του συμβάντος, μια αρχική κοινοποίηση στην οποία, κατά περίπτωση, αναφέρεται αν το περιστατικό προκλήθηκε πιθανώς από παράνομή ή κακόβουλή ενέργεια*».[357] Η Επιτροπή επιλέγει στην αναθεωρημένη οδηγία να προσδιορίσει το χρονικό διάστημα εντός του οποίου θα πρέπει να γίνει η κοινοποίηση προς του αρμόδιους χωρίς. Πλέον η έννοια της *«χωρίς αδικαιολόγητης καθυστέρησης»*

[353] Ibid *supra* 298, pp. 227-228.

[354] Ibid *supra* 311.

[355] Ibid *supra* 22, Άρθρο 20 της Πρότασης.

[356] Ibid *supra* 22, Άρθρο 20 της Πρότασης.

[357] Ibid *supra* 22, Άρθρο 20 της Πρότασης.

εξειδικεύεται σε χρονικό διάστημα εντός 24 ωρών από την στιγμή που γίνει αντιληπτό το συμβάν. Ακολούθως, σύμφωνα με το εδάφιο β' οι οντότητες θα πρέπει κατά τη εξέλιξη του συμβάντος να υποβάλουν ενδιάμεση έκθεση εάν υπάρχει σχετικό προς τούτο, αίτημα από την αρμόδια αρχή ή CSIRT.[358] Τέλος, σύμφωνα με το εδάφιο γ' οι οντότητες είναι υποχρεωμένες το αργότερο εντός ενός μηνός από το συμβάν να αποστείλουν τελική έκθεση, η οποία θα πρέπει να περιλαμβάνει τρία βασικά στοιχεία.[359] Πρώτον, «*λεπτομερή περιγραφή του περιστατικού, της σοβαρότητάς του και των επιπτώσεών του*». Δεύτερον, «*το είδος της απειλής ή τη βασική αιτία που ενδεχομένως προκάλεσε το περιστατικό»* και τρίτον *τα «εφαρμοζόμενα και εν εξέλιξη μέτρα μετριασμού».* Επί της ουσίας, η Επιτροπή επιθυμεί μέσω της τελικής έκθεσης αυτής, τη λογοδοσία των οντοτήτων για τον τρόπο χειρισμού των συμβάντων, ζητώντας συγκεκριμένα στοιχεία, προς αξιολόγησή τους.[360]

Η Επιτροπή προβλέπει έναν επιπλέον μηχανισμό με την εθελούσια κοινοποίηση. Ειδικότερα, σύμφωνα με το άρθρο 27 «*οι οντότητες που δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας οδηγίας μπορούν να υποβάλλουν κοινοποίηση, σε εθελοντική βάση, για σημαντικά συμβάντα, κυβερνοαπειλές ή παρ' ολίγον περιστατικά*».[361] Κατ' αυτόν τον τρόπο η Επιτροπή επιχειρεί να συμπεριλάβει στην αξιολόγηση των περιστατικών και αναφορές από οντότητες, οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής.[362] Αυτό έχει ως συνέπεια, να επαναξιολογούνται και τυχόν περιστατικά, τα οποία θα αποκλείονται άλλα θα συνέβαλλαν στην συνεκτίμηση τόσο

[358] Ibid *supra* 22, Άρθρο 20 της Πρότασης.

[359] Ibid *supra* 22, Άρθρο 20 της Πρότασης.

[360] Ibid *supra* 298, pp. 227-228.

[361] Ibis *supra* 22, Άρθρο 27 της Πρότασης.

[362] Ibid *supra* 298, pp. 229-230.

νέων επιθέσεων όσο και των επιπτώσεων με σκοπό την ενίσχυση του *«οπλοστασίου»* και των *«εργαλείων»* για καταπολέμηση του φαινομένου.[363]

(Γ) Εποπτεία και επιβολή κυρώσεων

Στην πρόταση της, η Επιτροπή προτείνει τη διαφοροποίηση στον τρόπο εποπτείας των βασικών και σημαντικών οντοτήτων[364]. Το άρθρο 29 της πρότασης καθορίζει την εποπτεία και επιβολή μέτρων όσον αφορά τις βασικές οντότητες και το άρθρο 30 της πρόταση ρυθμίζει την εποπτεία και επιβολή μέτρων όσο αφορά τις σημαντικές οντότητες.[365] Η εποπτεία των βασικών οντοτήτων δύναται να διενεργηθεί εκ των προτέρων και εκ των υστέρων.[366] Ειδικότερα, το άρθρο 29 παράγραφος 2 της πρότασης καταγράφει τα μέτρα που μπορούν να ληφθούν εκ των προτέρων για τις βασικές οντότητες.[367] Στην παράγραφο 4 του ίδιου άρθρου καθορίζονται τα μέτρα που επιβάλλονται εκ των υστέρων όταν δηλαδή μέσω αποδεικτικών γεγονότων ή και στοιχείων φανεί ότι οι βασικές οντότητες δεν πληρούν τις απαιτήσεις των άρθρων 18 και 20.[368] Αντίθετα, η εποπτεία των σημαντικών οντοτήτων γίνεται μόνο εκ των υστέρων.[369]Ειδικότερα, στο άρθρου 30 παράγραφος 4 καθορίζονται τα εποπτικά μέτρα που μπορούν να ληφθούν εκ των υστέρων με σκοπό τη συμμόρφωση των σημαντικών οντοτήτων με τις απαιτήσεις των άρθρων 18 και 20.[370] Εκ των ανωτέρω, ανακύπτει ότι οι βασικές οντότητες υπόκεινται σε ένα *«πλήρη»* εποπτικό έλεγχο ενώ

[363] Ibis *supra* 298, pp.229-230.

[364] Ibis *supra* 291.

[365] Ibid *supra* 298, pp. 229-230.

[366] Ibid *supra* 298, pp. 229-230.

[367] Ibid *supra* 22, Άρθρο 29 της Πρότασης.

[368] Ibid *supra* 298, pp. 228-229.

[369] Ibid *supra* 298, pp. 228-229.

[370] Ibid *supra* 22, Άρθρο 30 της Πρότασης.

οι σημαντικές οντότητες σε έναν πιο «*ελαφρύ»* εποπτικό έλεγχο.[371] Η διαφοροποίηση στον τρόπο εποπτείας των βασικών και σημαντικών οντοτήτων δεν είναι τυχαία. Η Επιτροπή προτείνει ένα πιο ολοκληρωμένο εποπτικό έλεγχο στις βασικές οντότητες λόγω της ήσσονος σημασίας τους στην εσωτερική αγορά, ως επεξηγήθηκε ανωτέρω. Συνεπώς, η έκθεση των βασικών οντοτήτων σε κινδύνους και απειλές δύναται να αποδιοργανώσει τα ίδια τα θεμέλια της εσωτερική αγορά της Ένωσης. Ενώ στις σημαντικές οντότητες, η Επιτροπή επιλέγει να είναι πιο *«χαλαρή»* η εποπτεία διότι γνωρίζει ότι οι συνέπειες της μη συμμόρφωσής τους, δεν θα έχουν το ίδιο αντίκτυπο με αυτό των βασικών οντοτήτων.[372]

Επιπλέον, όσο αναφορά τις βασικές οντότητες, σε περίπτωση που τα μέτρα επιβολής αποδειχθούν αναποτελεσματικά, σύμφωνα με το άρθρο 29 παράγραφος 5 της πρότασης, τα κράτη μέλη *«διασφαλίζουν ότι οι αρμόδιες αρχές έχουν την εξουσία να ορίσουν προθεσμία εντός της οποίας η βασική οντότητα καλείται να λάβει τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή τη συμμόρφωση με τις απαιτήσεις».*[373] Αν δεν συμμορφωθούν εντός της προβλεπόμενης προθεσμίας, τότε προβλέπονται επιπρόσθετα μέτρα επιβολής. Έως ότου ληφθούν τα αναγκαία μέτρα για την αποκατάσταση των ελλείψεων ή και συμμόρφωσης τους, είναι δυνατό να επιβληθούν κυρώσεις. Κυρώσεις στις βασικές οντότητές δύναται να επιβληθούν δυνάμει των παραγραφών 4 και 5 του άρθρου 29. Η παράγραφος 7 αναφέρεται στα κριτήρια που θα πρέπει να λάβουν υπόψη οι αρμόδιες αρχές πριν την επιβολή των εν λόγω κυρώσεων. Τα κριτήρια αυτά είναι τα ακόλουθα (α) η σοβαρότητα της παράβασης και η σημασία των διατάξεων που παραβιάστηκαν, (β) η διάρκεια της

[371] Ibis *supra* 298, pp. 228-229.

[372] Ibid *supra* 298, pp. 228-229.

[373] Ibid *supra* 22, Άρθρο 29 της Πρότασης.

παραβίασης, (γ) η πραγματική ζημία, (δ) το αν η παράβαση διαπράχθηκε εκ προθέσεως ή εξ αμέλειας, (δ) το αν η οντότητα έλαβε μέτρα για την πρόληψη ή και των μετριασμό της ζημίας ή και των απειλών, (στ) η τήρηση εκ μέρους της οντότητας εγκεκριμένων κωδίκων δεοντολογίας ή εγκεκριμένων μηχανισμών πιστοποίησης και (ζ) ο βαθμός συνεργασίας του υπαίτιου φυσικού ή νομικού προσώπου με τις αρμόδιες αρχές.[374] Συνεπώς, πριν την επιβολή των κυρώσεων, η Επιτροπή προτείνει να λαμβάνονται αντισταθμιστικοί παράγοντες υπόψη. Τα κριτήρια αυτά λαμβάνονται υπόψη και στις σημαντικές οντότητες, δυνάμει της παραγράφου 5 του άρθρου 30.

Περαιτέρω, η πρόταση προβλέπει στο άρθρο 29 παράγραφος 6 ότι *«κάθε φυσικό πρόσωπο που είναι υπεύθυνο ή ενεργεί ως αντιπρόσωπος βασικής οντότητας με βάση την εξουσία εκπροσώπησής της, την αρμοδιότητα να λαμβάνει αποφάσεις εξ ονόματός της ή να ασκεί τον έλεγχό της, έχει τις εξουσίες να διασφαλίζει τη συμμόρφωσή της με τις υποχρεώσεις που ορίζονται στην παρούσα οδηγία. Τα κράτη μέλη μεριμνούν ώστε τα εν λόγω φυσικά πρόσωπα να μπορούν να θεωρηθούν υπεύθυνα για παράβαση των καθηκόντων τους όσον αφορά την τήρηση των υποχρεώσεων που ορίζονται στην παρούσα οδηγία».*[375] Η διάταξη αυτή εγείρει δυο προβληματισμούς. Κατ' αρχήν σε ποια πρόσωπα αναφέρεται και κατ' δεύτερον εάν η ευθύνη είναι αστική ή και ποινική.[376] Συμπληρωματικά, η υποπαράγραφος β' της παραγράφου 5 του άρθρου 29 αναφέρει ότι *«οι αρμόδιες αρχές έχουν εξουσία να επιβάλουν ή να ζητήσουν από τα αρμόδια όργανα ή δικαστήρια να επιβάλουν, σύμφωνα με την εθνική νομοθεσία, προσωρινή απαγόρευση κατά οποιουδήποτε προσώπου ασκεί διευθυντικά καθήκοντα σε επίπεδο γενικού διευθυντή ή νομικού εκπροσώπου στην εν λόγω βασική*

[374] Ibid *supra* 22, Άρθρο 29 της Πρότασης.

[375] Ibid *supra* 22, Άρθρο 29 της Πρότασης.

[376] Ibid *supra* 298, pp. 229.

οντότητα, καθώς και οποιουδήποτε άλλου φυσικού προσώπου θεωρείται υπαίτιο για την παράβαση, να ασκούν διευθυντικά καθήκοντα στην εν λόγω οντότητας».[377] Συνεπώς, από το συνδυασμό των ανωτέρω διατάξεων φαίνεται ότι ευθύνη μπορεί να αποδοθεί πρώτον σε οποιοδήποτε πρόσωπο ασκεί διευθυντικά καθήκοντα σε επίπεδο γενικού διευθυντή ή νομικού εκπροσώπου και δεύτερον σε οποιοδήποτε φυσικό πρόσωπο που κριθεί υπαίτιος για παραβίαση.[378] Η παράγραφος 6 ισχύει κατ' αναλογία και στις σημαντικές οντότητες σύμφωνα με το άρθρο 30, παράγραφος 5. Ωστόσο, το άρθρο 29, παράγραφος 5 δεν τυγχάνει ανάλογης εφαρμογής στις σημαντικές οντότητές, θέτοντας τον προβληματισμό σε ποια φυσικά πρόσωπα θα αποδοθούν ευθύνες στις σημαντικές οντότητες, εφόσον δεν διευκρινίζονται.[379]Η απάντηση ενδέχεται να δοθεί μελλοντικά.

Επιπροσθέτως, η Επιτροπή προτείνει πιο δραστικές κυρώσεις και στις δύο οντότητες. Όπως αναφέρθηκε και στην αιτιολογική σκέψη της πρότασης, παρατηρήθηκε ότι τα κράτη μέλη είναι απρόθυμα να επιβάλουν κυρώσεις για τυχόν παραβιάσεις των διατάξεων της τρέχουσας οδηγίας.[380]Το γεγονός αυτό μπορεί να υπονομεύσει την αποτελεσματική επιδίωξη των στόχων της οδηγίας. Ειδικότερα, το άρθρο 21 της υπάρχουσας οδηγίας προβλέπει ότι *«τα κράτη μέλη είναι υπεύθυνα να επιβάλλουν κυρώσεις, οι οποίες πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές».*[381] Με την μη επιβολή κυρώσεων εκ μέρους των κρατών μελών αφενός δεν αποτρέπονται τέτοιες αδρανείς συμπεριφορές και αφετέρου γίνονται αποδεκτές. Περαιτέρω, ο μη σαφής προσδιορισμός των κυρώσεων έδωσε στα κράτη μέλη

[377] Ibid *supra* 22, Άρθρο 29 της Πρότασης.

[378] Ibid *supra* 298, pp. 229.

[379] Ibid *supra* 298, pp. 229.

[380] Ibid *supra* 22, (Βλ. Αιτιολογική Έκθεση).

[381] Ibid *supra* 50, Άρθρο 21 της Οδηγίας.

μεγάλη διακριτική ευχέρεια.[382] Η ευχέρεια αυτή οδήγησε σε διαφορετική πρακτική εφαρμογή μεταξύ των κρατών μελών σε σχέση με το είδος της ποινής και το ύψος. Για παράδειγμα, η Κύπρος και το Βέλγιο πέραν από χρηματικές κυρώσεις προβλέπουν και ποινές φυλάκισης.[383]

Για την εξάλειψη των εμποδίων, η Επιτροπή στο άρθρο 31 παράγραφο 4 προβλέπει ότι *«οι παραβάσεις των υποχρεώσεων που προβλέπονται στο άρθρο 18 ή στο άρθρο 20 υπόκεινται, σύμφωνα με τις παραγράφους 2 και 3 του παρόντος άρθρου, σε διοικητικά πρόστιμα κατ' ανώτατο όριο ύψους τουλάχιστον 10 000 000 EUR ή έως 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης στην οποία ανήκει η βασική ή σημαντική οντότητα κατά το προηγούμενο οικονομικό έτος, ανάλογα με το ποιο ποσό είναι υψηλότερο».*[384] Εν προκειμένω, η Επιτροπή καθορίζει πλέον ρητά το είδος των κυρώσεων που θα πρέπει να επιβάλλουν τα κράτη μέλη, καθώς και το ύψος αυτών, εν αντιθέσει με ότι ισχύει τη δεδομένη στιγμή σύμφωνα με το άρθρο 21 της τρέχουσας οδηγίας.[385] Επιπλέον, σύμφωνα με τους σχολιαστές οι εν λόγω διάταξη αυτή ομοιάζει αρκετά με το άρθρο 83 του Κανονισμού GDPR.[386]

(Δ) Αναφορά στον Κανονισμό GDPR

Η Επιτροπή στην αναθεωρημένη οδηγία ρυθμίζει και τις περιπτώσεις παραβίασης προσωπικών δεδομένων. Ειδικότερα, στο άρθρο 20 παράγραφος 4 της πρότασης, στην έννοια που περιστατικού που θεωρείται ως σημαντικό γίνεται πλέον αναφορά σε φυσικά πρόσωπα, τα οποία ενδέχεται να επηρεαστούν ή επηρεάστηκαν

[382] Ibid *supra* 108.

[383] Ibid *supra* 108.

[384] Ibid *supra* 22, Άρθρο 31 της Οδηγίας.

[385] Ibid *supra* 298, pp. 229.

[386] Ibid *supra* 298, pp. 229.

από το εν λόγω περιστατικό, προκαλώντας τους *«σημαντικές υλικές ή μη υλικές ζημίες»*.[387] Από την ανωτέρω διάταξη συνάγεται ότι η Επιτροπή επιθυμεί και προληπτικά να ληφθούν μέτρα από τις οντότητες πριν ακόμη υπάρξουν οι όποιες συνέπειες, ήτοι υλικές ή μη υλικές ζημίες. Αυτό συμβαίνει διότι με τη διαρροή των προσωπικών δεδομένων που υπάρχουν στις υπηρεσίες των οντοτήτων, λόγω κακόβουλων ή μη ενεργειών, δύνανται οι παραβάτες να χρησιμοποιούν ή και να εκμεταλλευτούν προσωπικές πληροφορίες πολιτών (π.χ. στοιχεία τραπεζικού λογαριασμού, ιατρικό ιστορικό κ.α.) για αλλότριους σκοπούς. Κατ' επέκταση, η Επιτροπή απαιτεί και σε αυτές τις περιπτώσεις οι αρμόδιες οντότητες να λάβουν όλα τα απαιτούμενα μέτρα για τη διαχείριση των ενδεχόμενων κινδύνων. Στην οδηγία ως έχει σήμερα παρατηρείται όπως ήδη σχολιάστηκε ένα νομοθετικό κενό ως προς τις περιπτώσεις αυτές.[388] Στον ορισμό της σοβαρής διατάραξης στην οδηγία NIS, δεν υπάρχει καμία αναφορά ως προς τις ζημίες που προκλήθηκαν ή ενδεχομένως να προκληθούν στα φυσικά πρόσωπα. Κατά συνέπεια οι αρμόδιες οντότητες δεν γνωρίζουν πως να αντιμετωπίσουν τις εν λόγω περιπτώσεις.

Συμπληρωματικά, στο άρθρο 33 της πρότασης προβλέπεται ότι *«εαν οι αρμόδιες αρχές έχουν ενδείξεις ότι η παράβαση από βασική ή σημαντική οντότητα των υποχρεώσεων που ορίζονται στα άρθρα 18 και 20 συνεπάγεται παραβίαση δεδομένων προσωπικού χαρακτήρα, όπως ορίζεται στο άρθρο 4 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 2016/679, η οποία κοινοποιείται σύμφωνα με το άρθρο 33 του εν λόγω κανονισμού, ενημερώνουν τις εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του εν λόγω κανονισμού εντός εύλογου χρονικού διαστήματος».*[389] Με

[387] Ibid *supra* 22, Άρθρο 20 της Οδηγίας.

[388] Ibid *supra* 24, pp. 101.

[389] Ibid *supra* 22, Άρθρο 33 της Πρότασης.

την ανωτέρω διάταξη, αποσαφηνίζει πλέον ότι οι αρμόδιες αρχές, στις ως άνω περιπτώσεις, θα πρέπει να συνεργάζονται άμεσα και στενά με τις εποπτικές αρχές ως αυτές καθορίζονται σύμφωνα με τον Κανονισμό GDPR. Η κοινοποίηση προς τις αρμόδιες εποπτικές αρχές θα πρέπει, ως επιτάσσει το γράμμα του άρθρου 33 του Κανονισμού GDPR, να λαμβάνει χώρα *«εντός 72 ωρών από τη* στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα».[390] Επομένως, από τη στιγμή της κοινοποίησης αναλαμβάνουν δράση οι αρμόδιες εποπτικές αρχές, σύμφωνα με τις διατάξεις του εν λόγω κανονισμού, για να διαφυλάξουν τα προσωπικά δεδομένα των φυσικών προσώπων που τελούν υπό κίνδυνο. Συνεπώς, οι αρμόδιες αρχές της αναθεωρημένης οδηγίας θα λάβουν τα απαιτούμενα μέτρα για τη προάσπιση και διαφύλαξη των υπηρεσιών των οντοτήτων και οι αρμόδιες εποπτικές αρχές του Κανονισμού GDPR θα λάβουν τα αναγκαία μέτρα για την διαφύλαξη των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων. Κατ' ακολουθίαν, οι διαδικασίες που θα ακολουθηθούν θα είναι ξεχωριστές και παράλληλες με πρωταρχικό σκοπό την εύρυθμη λειτουργία της εσωτερικής αγοράς.

Επιπλέον στο άρθρο 32 παράγραφος 2 της πρότασης αναφέρεται ότι *«εάν οι εποπτικές αρχές που είναι αρμόδιες σύμφωνα με τα άρθρα 55 και 56 του κανονισμού (ΕΕ) 2016/679 αποφασίσουν να ασκήσουν τις εξουσίες τους σύμφωνα με το άρθρο 58 στοιχείο θ) του εν λόγω κανονισμού και να επιβάλουν διοικητικό πρόστιμο, οι αρμόδιες αρχές δεν επιβάλλουν διοικητικό πρόστιμο για την ίδια παράβαση δυνάμει του άρθρου 31 της παρούσας οδηγίας. Οι αρμόδιες αρχές μπορούν, ωστόσο, να εφαρμόζουν τα μέτρα επιβολής ή να ασκούν τις εξουσίες επιβολής κυρώσεων που προβλέπονται στο άρθρο 29 παράγραφος 4 στοιχεία α) έως θ), στο άρθρο 29 παράγραφος 5 και στο*

[390] Ibid *supra* 198, Άρθρο 33 του Κανονισμού.

άρθρο 30 παράγραφος 4 στοιχεία α) έως η) της παρούσας οδηγίας».[391] Από την ανωτέρω διάταξη συνάγεται ότι για μια παραβίαση δεν μπορούν να συντρέξουν δύο διοικητικά πρόστιμα. Θα μπορούσε να αναρωτηθεί κανείς τι γίνεται τις περιπτώσεις που μια παραβίαση στο ένα νομοθετικό κείμενο ρυθμίζεται πιο αυστηρά επιβάλλοντας τσουχτερά πρόστιμα ενώ στο άλλο υπάρχουν πιο «χαλαρές» κυρώσεις. Ως προς το ζήτημα αυτό φαίνεται ότι η Επιτροπή επιλέγει, να υιοθετήσει στην αναθεωρημένη οδηγία τον ίδιο τρόπο ρύθμισης των προστίμων με αυτόν που ήδη καθορίζεται στον Κανονισμό GDPR. Όπως προαναφέρθηκε το άρθρο 31 της αναθεωρημένης οδηγίας ομοιάζει πολύ με το άρθρο 83 του Κανονισμού GDPR, αποκλείοντας με αυτό τον τρόπο τη σύγκρουση των διατάξεων μεταξύ τους. Ωστόσο, αυτό δεν αποκλείει τη δυνατότητα στις αρμόδιες εποπτικές αρχές να επιβάλλουν μέτρα επιβολής ως αυτά καθορίζονται στην αναθεωρημένη οδηγία. Περαιτέρω, από το άρθρο 32 της πρότασης επιτρέπεται για άλλες παραβιάσεις δυνάμει του Κανονισμού GDPR για τα οποία δεν επιβλήθηκαν πρόστιμα δυνάμει του άρθρου 31 της πρότασης, να επιβληθούν πρόσθετα πρόστιμα δυνάμει του Κανονισμού GDPR.[392] Συνεπώς από το συνδυασμό των ανωτέρω διατάξεων, γίνεται άμεσα πλέον αντιληπτό ότι τα δύο νομοθετικά κείμενα λειτουργούν ως συμπληρωματικά για τη ομαλή λειτουργία της Ένωσης.

Επίλογος

Η ραγδαία εξέλιξη της τεχνολογίας επηρεάζει τις κοινωνίες με δραματικό τρόπο. Το νομοθετικό πλαίσιο πρέπει να ακολουθεί για να αντιμετωπιστούν επαρκώς οι προκλήσεις αυτές της τεχνολογίας. Η αποτελεσματική αντιμετώπιση δε μπορεί

[391] Ibid *supra* 22, Άρθρο 32 της Πρότασης.

[392] Ibid supra 22, Άρθρο 32 της Πρότασης.

παρά να προκύπτει από παρεμβάσεις σε υπερεθνικό επίπεδο. Η Ευρωπαϊκή Επιτροπή και ο Ύπατος Εκπρόσωπος της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας ανακοίνωσαν το 2013 την επιτακτική ανάγκη οριοθέτησης σε ενωσιακό επίπεδο των απαιτήσεων κυβερνοασφάλειας για την διασφάλιση της εύρυθμης λειτουργίας της εσωτερικής αγοράς από τυχόν απειλές που ενδέχεται να κλονίσουν τις οικονομικές και κοινωνικές δραστηριότητές των ευρωπαίων πολιτών. Η πρώτη αυτή προσπάθεια οριζόντιας ρύθμισης επήλθε σε ένα χρονικό πλαίσιο, όπου η ανάγκη ρύθμισης ήταν άμεση και αναγκαία. Εντούτοις, τα νομοθετικά όργανα διαπραγματεύθηκαν επί της εν λόγω πρότασης 3 ολόκληρα χρόνια. Το εν λόγω διάστημα όλο και περισσότεροι ευρωπαίοι πολίτες και επιχειρήσεις στην επικράτεια της Ένωσης ήταν ευάλωτοι λόγω της μη ρύθμισης των εν λόγω ζητημάτων σε ενωσιακό επίπεδο. Εντέλει οι σχετικές νομοθετικές ρυθμίσεις τέθηκαν σε ισχύ το 2016. Το τελικό κείμενο που εγκρίθηκε ήταν πολύ πιο φτωχό από ότι η αρχική πρόταση της Επιτροπής.

Σκοπός της παρούσας εργασίας ήταν να εξετάσει κριτικά τις νομοθετικές ρυθμίσεις της εν λόγω οδηγία φέρνοντας στην επιφάνεια τις αδυναμίες της ως προς την επίτευξη ενός ομοιόμορφου και καθολικού αποτελέσματος κατά την εφαρμογή της από τα κράτη μέλη. Είδαμε λοιπόν, πρώτον ότι η υφιστάμενη οδηγία προσδιορίζει το πεδίο εφαρμογής της. Δεύτερον, οι οντότητες που εντάσσονται στο πεδίο εφαρμογής αυτής εξαρτώνται σε σημαντικό βαθμό από υποκειμενικά κριτήρια και τις επιλογές του κάθε κράτους μέλους. Τρίτον, παρέχει μεγάλη διακριτική ευχέρεια στα κράτη μέλη και στις οντότητες που εντάσσονται στο πεδίο εφαρμογής της για καίρια ζητήματα, τα οποία θα μπορούσε η ίδια η οδηγία να τα ρυθμίζει με ένα συγκεκριμένο τρόπο. Τέταρτον, η οδηγία εμπεριείχε ορισμένες ασαφείς έννοιες. Οι εν λόγω ασάφειες συνέβαλλαν και στην μη αποτελεσματική συνύπαρξη της με τον Κανονισμό

GDPR. Η έλλειψη σαφούς αναφοράς και οριοθέτησης της οδηγίας με τον Κανονισμό GDPR δείχνει κενά ως προς τη συνεργασία μεταξύ των εμπλεκόμενων μερών και την ανταλλαγή των πληροφορίων σχετικά με τον τρόπο αντιμετώπισης των περιστατικών από τα οποία μπορεί να διακυβεύεται η κυβερνοασφάλεια.

Δύο χρόνια μετά την πρακτική εφαρμογή της εν λόγω οδηγίας, η Ευρωπαϊκή Επιτροπή υπέβαλε πρόταση για κατάργηση της υφιστάμενης οδηγίας και θέσπισης νέας αναθεωρημένης οδηγίας. Η πρόταση της Επιτροπής αναγνωρίζει τα επιτεύγματα της πρώτης προσπάθειας, εντούτοις λαμβάνει υπόψη και τις εγγενείς αδυναμίες. Ως εκ τούτου, προτείνει την κατάργηση της διάκρισης των οντοτήτων σε φορείς εκμετάλλευσης βασικών υπηρεσιών και σε παρόχους ψηφιακών υπηρεσιών και την κατηγοριοποίηση των οντοτήτων σε σημαντικές και βασικές οντότητες. Η επιλογή της διάκρισης των οντοτήτων σε βασικές και σημαντικές αντικατοπτρίζει την σημασία των οντοτήτων αυτών στη λειτουργία της εσωτερικής αγοράς. Περαιτέρω, επεκτείνει το πεδίο εφαρμογής της οδηγίας εντάσσοντας πρόσθετους τομείς και υποτομείς. Επίσης, εντάσσονται και υπό ορισμένες προϋποθέσεις και οι μικρές και πολύ μικρές οντότητες διευρύνοντας έτσι σημαντικά το πεδίο εφαρμογής της σχετικής νομοθεσίας. Επιπλέον, εισάγει ένα αντικειμενικό κριτήριο για την ένταξη των εν λόγω οντοτήτων. Κατ' αυτόν τον τρόπο επιχειρεί να διασφαλίσει ότι θα ενταχθεί σε αυτή τη δεύτερη προσπάθεια ένα σημαντικό μέρος της οικονομίας της Ένωσης, το οποίο θα κατέχει τους αναγκαίους οικονομικούς και ανθρώπινους πόρους προς επίτευξη των στόχων της αναθεωρημένης οδηγίας.

Συν τοις άλλοις, διευρύνει και την έννοια του περιστατικού και περιλαμβάνει και τις συνέπειες και επιπτώσεις σε φυσικά πρόσωπα. Κατ' αυτόν τον τρόπο συνδέει την αναθεωρημένη οδηγία με τον Κανονισμό GDPR. Αξιοσημείωτο επίσης, το ότι καθορίζει την απαίτηση για συνεργασία της αναθεωρημένης οδηγίας με τον

Κανονισμό GDPR. Επιπροσθέτως, ως προς τις απαιτήσεις ασφάλειας και αναφοράς περιστατικών αναγνωρίζει ότι παραχωρήθηκε υπερβολική διακριτική ευχέρεια και προτείνει την επιβολή εποπτικών μέτρων εκ των προτέρων και εκ των υστέρων αναφορικά με τις απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών. Μεταξύ άλλων, εισάγει ευθύνες και σε φυσικά πρόσωπα λόγω μη συμμόρφωσης στις απαιτήσεις ασφάλειας και κοινοποίησης περιστατικών αναφοράς.

Υπό το φως των ανωτέρω προτεινόμενων αλλαγών, η δεύτερη προσπάθεια της Ευρωπαϊκής Επιτροπής ενδέχεται να είναι πιο αποτελεσματική ως προς την επιδίωξη των στόχων της Ενωσιακής νομοθεσίας. Ως προς το νομοθετικό κείμενο θα ήταν προτιμότερο αν η Ευρωπαϊκή Επιτροπή επέλεγε τη ρύθμιση των ως άνω ζητημάτων μέσω ενός κανονισμού. Κατ' αυτόν τον τρόπο θα διασφαλιζόταν το άμεσο των ρυθμίσεων της από τα κράτη μέλη. Πρέπει πάντως να έχουμε υπόψη μας ότι η διασφάλιση της κυβερνοασφάλειας είναι ένας διαρκής στόχος αφού η εξέλιξη της τεχνολογίας είναι διαρκής και επομένως και οι κίνδυνοι που γεννιούνται μπορεί συνεχώς να αλλάζουν. Κατά συνέπεια η αποτελεσματική αντιμετώπιση των κινδύνων του κυβερνοχώρου επιτάσσει μια περιοδική εξέταση, επαναξιολόγηση και ενδεχομένως τροποποίηση των νομικών και άλλων μέσων που υιοθετούμε προς αυτόν το σκοπό.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Αρθρογραφία

1. Ε. Βαγενά, «Το νέο θεσμικό πλαίσιο για την καταπολέμηση του κυβερνοεγκλήματος», *Νομική Βιβλιοθήκη*, ΔΙΤΕ (π. ΔΙΜΕΕ) , Τεύχος 1/2017, 2017, σελ. 18.

2. Κ. Πιπύρος, Λ. Μήτρου, «Κυβερνοεπίθεση ή κυβερνοπόλεμος;», *Νομική Βιβλιοθήκη*, ΔΙΤΕ (π. ΔΙΜΕΕ), Τεύχος 2/2018, 2018, σελ. 192.

Αγγλική Αρθρογραφία

1. T .Aleksandrowicz «The Act on the National Cybersecurity System as an Implementation of the NIS Directive», *Internal Security*, 2020, Vol. 12 Issue 1, p179-193.

2. I. Angeli/ E. Sieber-Fazakas, «Automotive Sector Within the Scope of Planned NIS II Cybersecurity Rules», *Budapest Business Journal*, 2021, Vol. 29, Issue 10, p13.

3. B. Calle «Supporting cybersecurity: The NIS Directive», *agendaNi*, 2018, Issue 91, p. 82.

4. S. Cassotta, M. Pettersson, «Climate change, environmental threats and cyber-threats to critical infrastructures in multi-regulatory sustainable global approach with sweden as an example», *Beijing Law Review*, 2019, Vol. 10, No. 3, pp. 635-636.

5. M. D. Cole, «Recent developments and overview of the country and practitioner's reports», *European Data Protection Law Review (EDPL)*, 2021, Vol 7, No. 1, pp. 91-93.

6. A. Cormack, «NISD2: A Common Framework for Information Sharing among Network Defenders», *SCRIPTed: A Journal of Law, Technology and Society*, Vol. 18, No. 1, 2021, pp. 83-98.

7. L. Grigoriadis, «Cybersecurity Insurance and New EU Cybersecurity and Data Protection Rules», *Business Law Review*, 2017, Vol. 38 Issue 6, p210-218.

8. M.T. Holzleitner, J. Reichl, «European provisions for cyber security in the smart grid – an overview of the NIS-directive», *Elektrotechnik Und Informationstechnik*, Vol 134, No. 1, 2017, pp. 14-18.

9. M.T. Holzieitner, J. Reichl, «Legal Problems for the Protection of Smart Grids from Cyber Threats», *European Energy Journal*, Vol. 6, Issue 3, 2016, pp. 53-61.

10. W. Long, «What's in the EU NIS Directive?», Computer Weekly, 2014, pp. 13.

11. L. Maglaras, G. Drivas, K. Noou, S. Rallis, «NIS directive: The case of Greece» *EAI Endorsed Transactions on Security* and Safety, Vol 4, Issue 14 , 2018, pp 1-5.

12. D. Markopoulou, V. Papakonstantinou, P. de Hert «The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation», *Computer law & security review,* Vol. 35, Issue 6, 2019, pp. 1-11.

13. J.D. Michels, I. Walden, «Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?», *European Law Review*, 2020, Vol. 45, Issue 1, p. 25-47.

14. A. Popescu, «The right to information and cybersecurity», *Journal of Law and Public Administration*, Vol. 3, No. 6, 2017, pp. 105-111.

15. N. Saqib, V. Germanos, Z. Wen, L. Maglaras, «Mapping of the Security Requirements of GDPR and NIS», *EAI Endorsed Transactions on Security & Safety* , 2020, Vol. 7, Issue 24, p1-18.

16. S. Schmitz-Berndt, F. Anheier, «Synergies in Cybersecurity Incident Reporting - The NIS Cooperation Group Publication 04/20 in Context», *European Data Protection Law Review*, 2021, Vol. 7 Issue 1, p101-107.

17. S. Schmitz-Berndt/ S. Schiffner, «Don't Put the Cart Before the Horse – Effective Incident Handling Under GDPR and NIS Directive», *IFIP International Summer School on Privacy and Identity Management*, Privacy and Identity, 2020, pp 3-17.

18. S. Schmitz-Berndt, S. Schiffner, «Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR», *International Review of Law, Computers & Technology*, 2021, Vol 35, No. 2, pp.101-115.

19. T. Siever «Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations», *International Cybersecurity Law Review*, 2021, pp. 1-9.

20. D. Stefanoudi «The Relevance and Applicability of Cybersecurity Laws with Regard to Data Storage on Board Satellites and on the Ground», *Air and Space Law*, Volume 44, Issue 4/5, 2019, pp. 425 – 444.

21. G. Szpor, «The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland», *Review of European and Comparative Law*, Vol 46, Issue 3, 2021, pp. 219-235.

22. C. Walker-Osborn, N. Patel, «EU Cybersecurity Directive», *Oxford University Press*, 2014, pp. 38-39.

23. R. Wilson; S. J. Shine, «Is Your Data Protected? A Look at Cybersecurity Regulations in the US and EU», *International In-House Counsel Journal*, Vol 10, No. 40, 2017, pp. 1-18.

<u>Διαδικτυακές Πηγές</u>

1. C. Haid, F. Schneider «Cybersecurity on the rise: The NIS Directive 2.0», Schonherr, Πρόσβαση 15/11/2021.

https://www.schoenherr.eu/content/cybersecurity-on-the-rise-the-nis-directive-2-0/

2. N. V. Tieghem, N. Lefebvre, «While preparing the NIS 2, update of the European overview of NIS transposition by the Member States…toward convergence?», RiskInsight , Πρόσβαση 1/11/2021.

https://www.riskinsight-wavestone.com/en/2021/09/en-pleine-preparation-de-la-nis-v2-mise-a-jour-du-tour-dhorizon-europeen-de-transposition-de-la-directive-nis-par-les-etats-membres-vers-une-convergence/

3. Ευρωπαϊκή Επιτροπή, Αντιπροσωπεία στην Ελλάδα «Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων». Πρόσβαση 1/10/2021

https://ec.europa.eu/greece/news/20201216____5_el

4. Πρόταση Ευρωπαϊκής Επιτροπής «Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148», ημερομηνίας 16/12/2020. Πρόσβαση 5/11/2021.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52020PC0823

5. Πρόταση Ευρωπαϊκής Επιτροπής «Πρόταση ΟΔΗΓΙΑ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση», ημερομηνίας 2/2/2013. Πρόσβαση 5/11/2021.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A52013PC0048

6. Σύσταση Ευρωπαϊκής Επιτροπής «Σύσταση της Επιτροπής, της 6ης Μαΐου 2003, σχετικά με τον ορισμό των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων», ημερομηνίας 6/5/2003. Πρόσβαση 5/11/2021.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CElEX:32003H0361

Νομοθεσία της Ένωσης

1. Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια).

https://eur-lex.europa.eu/legal-content/el/ALL/?uri=CELEX:32019R0881

2. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679

3. Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L1148