III

(Προπαρασκευαστικές πράξεις)

ΕΥΡΩΠΑΪΚΗ ΚΕΝΤΡΙΚΗ ΤΡΑΠΕΖΑ

ΓΝΩΜΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΕΝΤΡΙΚΗΣ ΤΡΑΠΕΖΑΣ

της 4ης Ιουνίου 2021

όσον αφορά πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα

(CON/2021/20)

(2021/C 343/01)

Εισαγωγή και νομική βάση

Στις 22, 23 και 29 Δεκεμβρίου 2020 η Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) έλαβε αίτημα από το Συμβούλιο της Ευρωπαϊκής Ένωσης και το Ευρωπαϊκό Κοινοβούλιο για τη διατύπωση γνώμης όσον αφορά, αντίστοιχα, πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014 ([1]) (εφεξής ο «προτεινόμενος κανονισμός») και πρόταση οδηγίας για την τροποποίηση των οδηγιών 2006/43/ΕΚ, 2009/65/ΕΚ, 2009/138/ΕΚ, 2011/61/ΕΕ, 2013/36/ΕΕ, 2014/65/ΕΕ, (ΕΕ) 2015/2366 και (ΕΕ) 2016/2341 ([2]) (εφεξής η «προτεινόμενη τροποποιητική οδηγία», από κοινού με τον προτεινόμενο κανονισμό, οι «προτεινόμενες πράξεις»).

Η γνωμοδοτική αρμοδιότητα της ΕΚΤ βασίζεται στο άρθρο 127 παράγραφος 4 και στο άρθρο 282 παράγραφος 5 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, δεδομένου ότι οι προτεινόμενες πράξεις περιέχουν διατάξεις που εμπίπτουν στους τομείς αρμοδιότητας της ΕΚΤ, ιδίως στη χάραξη και εφαρμογή νομισματικής πολιτικής, την προώθηση της ομαλής λειτουργίας των συστημάτων πληρωμών, τη συμβολή στην εκ μέρους των αρμόδιων αρχών ομαλή άσκηση πολιτικών που αφορούν τη σταθερότητα του χρηματοπιστωτικού συστήματος της αγοράς, καθώς και στα καθήκοντα της ΕΚΤ που αφορούν την προληπτική εποπτεία των πιστωτικών ιδρυμάτων βάσει του άρθρου 127 παράγραφος 2 πρώτη και τέταρτη περίπτωση και του άρθρου 127 παράγραφοι 5 και 6 της Συνθήκης. Η παρούσα γνώμη εκδόθηκε από το διοικητικό συμβούλιο, σύμφωνα με το άρθρο 17.5 πρώτη πρόταση του εσωτερικού κανονισμού της Ευρωπαϊκής Κεντρικής Τράπεζας.

1. **Γενικές παρατηρήσεις**

1.1 Η ΕΚΤ χαιρετίζει τον προτεινόμενο κανονισμό, ο οποίος αποσκοπεί στην ενίσχυση της κυβερνοασφάλειας και της επιχειρησιακής ανθεκτικότητας του χρηματοοικονομικού τομέα. Ειδικότερα, η ΕΚΤ χαιρετίζει τον σκοπό του προτεινόμενου κανονισμού που αφορά την εξάλειψη των φραγμών στην εσωτερική αγορά χρηματοπιστωτικών υπηρεσιών και τη διευκόλυνση της εδραίωσης και λειτουργίας της μέσω της εναρμόνισης των κανόνων που εφαρμόζονται στους τομείς της διαχείρισης κινδύνων των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ), της αναφοράς, των δοκιμών και του κινδύνου τρίτων παρόχων ΤΠΕ. Περαιτέρω, η ΕΚΤ χαιρετίζει τον σκοπό του προτεινόμενου κανονισμού που αφορά τον εξορθολογισμό και την εναρμόνιση τυχόν αλληλοεπικαλυπτόμενων κανονιστικών απαιτήσεων ή εποπτικών προσδοκιών στις οποίες υπόκεινται επί του παρόντος οι χρηματοπιστωτικές οντότητες βάσει του ενωσιακού δικαίου.

1.2 Η ΕΚΤ αντιλαμβάνεται ότι ως προς τις χρηματοπιστωτικές οντότητες που προσδιορίζονται ως φορείς εκμετάλλευσης βασικών υπηρεσιών ([3]) ο προτεινόμενος κανονισμός αποτελεί τομεακή νομική πράξη (lex specialis) κατά την έννοια του άρθρου 1 παράγραφος 7 της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]) (εφεξής η «οδηγία NIS»)· αυτό σημαίνει ότι οι απαιτήσεις που θεσπίζονται με τον προτεινόμενο κανονισμό υπερισχύουν, κατ' αρχήν, της οδηγίας NIS. Πρακτικά, οι χρηματοπιστωτικές οντότητες που προσδιορίζονται ως φορείς εκμετάλλευσης βασικών υπηρεσιών ([5]) κοινοποιούν, μεταξύ άλλων, συμβάντα σύμφωνα με τον προτεινόμενο

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Βλέπε άρθρο 1 παράγραφος 2 του προτεινόμενου κανονισμού.
([4]) 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 (ΕΕ L 194 της 19.7.2016, σ. 1).
([5]) Βλέπε άρθρο 5 της οδηγίας NIS.

κανονισμό και όχι με την οδηγία NIS. Μολονότι η ΕΚΤ χαιρετίζει τη μείωση ενδεχόμενων αλληλοεπικαλυπτόμενων απαιτήσεων για χρηματοπιστωτικές οντότητες στον τομέα της κοινοποίησης συμβάντων, πρέπει να εξεταστεί περαιτέρω η αλληλεπίδραση μεταξύ του προτεινόμενου κανονισμού και της οδηγίας NIS. Για παράδειγμα, ορισμένος τρίτος πάροχος υπηρεσιών ΤΠΕ ([6]) θα μπορούσε να υπόκειται βάσει του προτεινόμενου κανονισμού στις συστάσεις που διατυπώνει ο κύριος εποπτικός φορέας ([7]). Παράλληλα, ο ίδιος τρίτος πάροχος υπηρεσιών ΤΠΕ ενδέχεται να χαρακτηρίζεται ως φορέας εκμετάλλευσης βασικών υπηρεσιών βάσει της οδηγίας NIS και να υπόκειται στις δεσμευτικές οδηγίες που εκδίδει η αρμόδια αρχή ([8]). Σε μια τέτοια περίπτωση, ο τρίτος πάροχος υπηρεσιών ΤΠΕ θα μπορούσε να υπόκειται σε αντικρουόμενες συστάσεις οι οποίες διατυπώνονται βάσει του προτεινόμενου κανονισμού και σε δεσμευτικές οδηγίες οι οποίες εκδίδονται βάσει της οδηγίας NIS. Η ΕΚΤ προτείνει στα νομοθετικά όργανα της Ένωσης να εξετάσουν περαιτέρω τυχόν ανακολουθίες μεταξύ του προτεινόμενου κανονισμού και της οδηγίας NIS, οι οποίες ενδέχεται να παρακωλύουν την εναρμόνιση και τη μείωση των αλληλοεπικαλυπτόμενων και αντικρουόμενων απαιτήσεων για τις χρηματοπιστωτικές οντότητες.

1.3 Η ΕΚΤ αντιλαμβάνεται επίσης ότι βάσει της πρότασης οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148 ([9]) (εφεξής η «προτεινόμενη οδηγία NIS2»), τα «παρ' ολίγον περιστατικά» ([10]) υπόκεινται σε υποχρεώσεις αναφοράς ([11]). Μολονότι η αιτιολογική σκέψη 39 της προτεινόμενης οδηγίας NIS2 αναφέρεται στην έννοια του όρου «παρ' ολίγον περιστατικά», εντούτοις δεν είναι σαφές εάν η πρόθεση είναι να απαιτείται από τις χρηματοπιστωτικές οντότητες που απαριθμούνται στο άρθρο 2 του προτεινόμενου κανονισμού να αναφέρουν τα παρ' ολίγον περιστατικά. Συναφώς, και λαμβανομένου επίσης υπόψη του γεγονότος ότι τα παρ' ολίγον περιστατικά μπορούν να χαρακτηρίζονται ως τέτοια μόνον αφού λάβουν χώρα, η ΕΚΤ θα επιθυμούσε να λαμβάνει έγκαιρα κοινοποίηση των σημαντικών παρ' ολίγον περιστατικών, όπως ισχύει επί του παρόντος για τα περιστατικά κυβερνοασφάλειας. Η ΕΚΤ προτείνει καλύτερο συντονισμό μεταξύ του προτεινόμενου κανονισμού και της προτεινόμενης οδηγίας NIS2 προκειμένου να αποσαφηνιστεί το ακριβές πεδίο αναφοράς στο οποίο ενδέχεται να εμπίπτει ορισμένη χρηματοπιστωτική οντότητα δυνάμει των εν λόγω δύο διακριτών αλλά συνδεδεμένων νομοθετημάτων της Ένωσης. Παράλληλα, απαιτείται να καθοριστούν τα «παρ' ολίγον περιστατικά» και να προβλεφθούν ρυθμίσεις που θα διευκρινίζουν τη σημασία τους.

1.4 Η ΕΚΤ χαιρετίζει την παροχή κινήτρων στις χρηματοπιστωτικές οντότητες για τον διαμοιρασμό, σε εθελοντική βάση, απόρρητων πληροφοριών για την αντιμετώπιση κυβερνοαπειλών με σκοπό την ενίσχυση και την υποστήριξη των θέσεών τους σχετικά με την κυβερνοανθεκτικότητα. Η ΕΚΤ έχει συμβάλει στην υλοποίηση της πρωτοβουλίας με γνώμονα την αγορά «Cyber threat Intelligence Information Sharing Initiative (CIISI-EU)», ενώ έχει διαθέσει τα σχέδια για οποιονδήποτε επιθυμεί να αναπτύξει και να στηρίξει μια τέτοια πρωτοβουλία ([12]).

1.5 Η ΕΚΤ υποστηρίζει τη συνεργασία μεταξύ των αρμόδιων αρχών για τους σκοπούς του προτεινόμενου κανονισμού, των ευρωπαϊκών εποπτικών αρχών (ΕΕΑ) και των ομάδων απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRTS) ([13]). Είναι σημαντική η ανταλλαγή πληροφοριών προκειμένου να εξασφαλιστεί η επιχειρησιακή ανθεκτικότητα της Ένωσης, καθώς η ανταλλαγή πληροφοριών και η συνεργασία μεταξύ των αρχών μπορεί να συμβάλει στην αποφυγή κυβερνοεπιθέσεων και να συντελέσει στη μείωση της εξάπλωσης απειλών ΤΠΕ. Θα πρέπει να προαχθεί μια ενιαία αντίληψη των κινδύνων που σχετίζονται με τις ΤΠΕ και να εξασφαλιστεί η συνεπής αξιολόγησή τους στην Ένωση. Είναι ύψιστης σημασίας να κοινοποιούνται οι πληροφορίες στο ενιαίο κέντρο επαφής ([14]) και στις εθνικές CSIRTS από τις αρμόδιες αρχές ([15]) μόνον όταν υφίστανται σαφώς θεσπισμένοι μηχανισμοί ταξινόμησης και ανταλλαγής πληροφοριών, σε συνδυασμό με επαρκείς εγγυήσεις για την εξασφάλιση της εμπιστευτικότητας.

1.6 Τέλος, η ΕΚΤ χαιρετίζει τη θέσπιση κανόνων για τη διατήρηση των δεδομένων προσωπικού χαρακτήρα και δεδομένων βάσει του προτεινόμενου κανονισμού. Για τη διάρκεια της περιόδου διατήρησης θα πρέπει να ληφθούν υπόψη η έρευνα, η επιθεώρηση, το αίτημα παροχής πληροφοριών, η κοινοποίηση, η δημοσίευση, η αξιολόγηση, η επαλήθευση, η εκτίμηση και η κατάρτιση των σχεδίων επίβλεψης ή εποπτείας που ενδέχεται να πρέπει να εκτελούν οι αρμόδιες αρχές στο πλαίσιο των οικείων υποχρεώσεων και καθηκόντων τους βάσει του προτεινόμενου κανονισμού. Εν προκειμένω θεωρείται επαρκής μια περίοδος διατήρησης διάρκειας 15 ετών. Η περίοδος διατήρησης των δεδομένων θα μπορούσε να συντμηθεί ή να παραταθεί, αναλόγως των ειδικών περιστάσεων. Εν

([6]) Βλέπε άρθρο 3 παράγραφος 15 του προτεινόμενου κανονισμού.
([7]) Βλέπε άρθρο 31 παράγραφος 1 στοιχείο δ) του προτεινόμενου κανονισμού.
([8]) Βλέπε άρθρο 15 παράγραφος 3 της οδηγίας NIS.
([9]) COM(2020) 823 final.
([10]) Γεγονότα τα οποία θα μπορούσαν δυνητικά να προκαλέσουν βλάβη, αλλά των οποίων η συντέλεση εμποδίστηκε επιτυχώς· βλέπε αιτιολογική σκέψη 39 της οδηγίας NIS2.
([11]) Βλέπε άρθρο 11 της οδηγίας NIS2.
([12]) «Cyber threat Intelligence Information Sharing Initiative (CIISI-EU)», διαθέσιμο στον ιστότοπο της ΕΚΤ (www.ecb.europa.eu).
([13]) Βλέπε άρθρο 42 του προτεινόμενου κανονισμού.
([14]) Βλέπε άρθρο 8 παράγραφος 3 της οδηγίας NIS.
([15]) Βλέπε επίσης άρθρα 11, 26 και 27 της οδηγίας NIS2.

προκειμένω η ΕΚΤ προτείνει στα νομοθετικά όργανα της Ένωσης, κατά τη διαμόρφωση της οικείας ρύθμισης για τη διατήρηση των δεδομένων προσωπικού χαρακτήρα και των δεδομένων, να λαμβάνουν επίσης υπόψη την αρχή της ελαχιστοποίησης των δεδομένων, καθώς και την περαιτέρω επεξεργασία για λόγους αρχειοθέτησης που άπτονται του δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς ([16]).

2. **Ειδικές παρατηρήσεις σχετικά με την επίβλεψη, καθώς και με τον συμψηφισμό και τον διακανονισμό αξιογράφων**

2.1 *Καθήκοντα επίβλεψης του ΕΣΚΤ και του Ευρωσυστήματος*

2.1.1 Η Συνθήκη και το καταστατικό του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών και της Ευρωπαϊκής Κεντρικής Τράπεζας (εφεξής το «καταστατικό του ΕΣΚΤ») ορίζουν ότι το Ευρωσύστημα ασκεί την επίβλεψη των συστημάτων συμψηφισμού και πληρωμών ως δραστηριότητα στενά συνδεόμενη με τα βασικά καθήκοντα νομισματικής πολιτικής που το ίδιο υπέχει. Σύμφωνα με το άρθρο 127 παράγραφος 2 τέταρτη περίπτωση της Συνθήκης, όπως αντικατοπτρίζεται στο άρθρο 3 παράγραφος 1 του καταστατικού του ΕΣΚΤ, ένα από τα βασικά καθήκοντα που ασκούνται μέσω του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών (ΕΣΚΤ) είναι η προώθηση της ομαλής λειτουργίας των συστημάτων πληρωμών. Κατά την άσκηση αυτού του βασικού καθήκοντος η ΕΚΤ και οι εθνικές κεντρικές τράπεζες μπορούν να παρέχουν διευκολύνσεις, και η ΕΚΤ μπορεί να θεσπίζει κανονισμούς με σκοπό την εξασφάλιση αποτελεσματικών και υγιών συστημάτων συμψηφισμού και πληρωμών, εντός της Κοινότητας και με άλλες χώρες ([17]). Στο πλαίσιο του ρόλου επίβλεψης που ασκεί η ΕΚΤ εξέδωσε τον κανονισμό (ΕΕ) αριθ. 795/2014 της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ/2014/28) (εφεξής ο «κανονισμός ΣΣΣΠ») ([18]). Ο κανονισμός ΣΣΣΠ εφαρμόζει επιτακτικά τις αρχές για τις υποδομές χρηματοπιστωτικής αγοράς του Απριλίου 2012 που εξέδωσε η επιτροπή συστημάτων πληρωμών και διακανονισμού και ο διεθνής οργανισμός επιτροπών κινητών αξιών ([19]), οι οποίες είναι νομικά δεσμευτικές και καλύπτουν τόσο τα συστημικώς σημαντικά συστήματα πληρωμών μεγάλης αξίας όσο και τα μικρής αξίας που τελούν υπό τη διαχείριση κεντρικής τράπεζας του Ευρωσυστήματος ή ιδιωτικής οντότητας. Το πλαίσιο του Ευρωσυστήματος για την πολιτική επίβλεψης (Eurosystem oversight policy framework) ([20]) καθορίζει τα μέσα πληρωμών ως «αναπόσπαστο μέρος των συστημάτων πληρωμών» και, ως εκ τούτου, τα συμπεριλαμβάνει στο πεδίο της επίβλεψής του. Το πλαίσιο αυτό όσον αφορά τα μέσα πληρωμής τελεί υπό αναθεώρηση ([21]). Σύμφωνα με το πλαίσιο αυτό, ένα μέσο πληρωμής (π.χ. κάρτα, μεταφορά κεφαλαίων, άμεση χρέωση, μεταφορά ηλεκτρονικού χρήματος και ψηφιακό κέρμα πληρωμών ([22])) ορίζεται ως εξατομικευμένη συσκευή (ή σύνολο συσκευών) και/ή σύνολο διαδικασιών που συμφωνούνται μεταξύ χρήστη και παρόχου υπηρεσιών πληρωμών και χρησιμοποιούνται για την κίνηση μεταφοράς αξίας ([23]).

2.1.2 Υπό το πρίσμα των παραπάνω, η ΕΚΤ επικροτεί την εξαίρεση από το πεδίο εφαρμογής του προτεινόμενου κανονισμού των διαχειριστών συστήματος κατά τον ορισμό του άρθρου 2 στοιχείο ιστ) της οδηγίας 98/26/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([24]), των συστημάτων πληρωμών (συμπεριλαμβανομένων όσων τελούν υπό τη διαχείριση κεντρικών τραπεζών), των καθεστώτων πληρωμών και των ρυθμίσεων πληρωμών, λαμβανομένης υπόψη της

([16]) Βλέπε άρθρο 4 παράγραφος 1 στοιχείο β) και άρθρο 13 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

([17]) Βλέπε άρθρο 22 του καταστατικού του ΕΣΚΤ.

([18]) Κανονισμός (ΕΕ) αριθ. 795/2014 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 3ης Ιουλίου 2014, σχετικά με τις απαιτήσεις επίβλεψης για τα συστημικώς σημαντικά συστήματα πληρωμών (ΕΚΤ/2014/28) (ΕΕ L 217 της 23.7.2014, σ. 16).

([19]) Διαθέσιμο στον ιστότοπο της Τράπεζας Διεθνών Διακανονισμών (www.bis.org).

([20]) «Eurosystem oversight policy framework», αναθεωρημένη έκδοση (Ιούλιος 2016), διαθέσιμη στον ιστότοπο της ΕΚΤ (www.ecb.europa.eu).

([21]) Βλέπε την αναθεωρημένη και ενοποιημένη έκδοση του «Eurosystem oversight framework for electronic payment instruments, schemes and arrangements», Οκτωβρίου 2020 (εφεξής το «πλαίσιο PISA»), διαθέσιμη στον ιστότοπο της ΕΚΤ (www.ecb.europa.eu).

([22]) Το ψηφιακό κέρμα πληρωμών αποτελεί ψηφιακή αναπαράσταση αξίας η οποία υποστηρίζεται από απαιτήσεις ή περιουσιακά στοιχεία που καταχωρίζονται αλλού και επιτρέπει τη μεταφορά αξίας μεταξύ τελικών χρηστών. Ανάλογα με την υποκείμενη σχεδίασή τους, τα ψηφιακά κέρματα πληρωμών μπορούν να προβλέπουν μεταφορά αξίας χωρίς τη μεσολάβηση οπωσδήποτε κεντρικού τρίτου φορέα και/ή χρήση λογαριασμών πληρωμής.

([23]) Ως «μεταφορά αξίας» νοείται η πράξη που εκκινεί από τον πληρωτή, για λογαριασμό αυτού ή από τον δικαιούχο της πληρωμής, με την οποία πραγματοποιείται μεταφορά χρημάτων ή ψηφιακών κερμάτων πληρωμών ή κατάθεση/ανάληψη μετρητών σε/από λογαριασμό χρήστη, ανεξάρτητα από τυχόν υποκείμενες υποχρεώσεις μεταξύ πληρωτή και δικαιούχου. Η μεταφορά μπορεί να περιλαμβάνει έναν ή περισσότερους παρόχους υπηρεσιών πληρωμών. Ο ορισμός της «μεταφοράς αξίας» βάσει του πλαισίου PISA αποκλίνει από τον ορισμό των «χρηματικών ποσών» κατά την οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35). Μια «μεταφορά αξίας» στο πλαίσιο «μέσου πληρωμών» όπως ορίζεται στην εν λόγω οδηγία μπορεί να αναφέρεται μόνο σε μεταφορά «χρηματικών ποσών». Σύμφωνα με την εν λόγω οδηγία, τα «χρηματικά ποσά» δεν περιλαμβάνουν ψηφιακά κέρματα πληρωμών, εκτός εάν τα ψηφιακά κέρματα μπορούν να ταξινομηθούν ως ηλεκτρονικό χρήμα (ή υποθετικά ως λογιστικό χρήμα).

([24]) Οδηγία 98/26/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Μαΐου 1998, σχετικά με το αμετάκλητο του διακανονισμού στα συστήματα πληρωμών και στα συστήματα διακανονισμού αξιογράφων (ΕΕ L 166 της 11.6.1998, σ. 45).

εφαρμογής των προαναφερθέντων πλαισίων επίβλεψης. Για τους λόγους αυτούς, τα καθήκοντα που ανατίθενται στο ΕΣΚΤ δυνάμει της Συνθήκης και τα καθήκοντα που ανατίθενται στο Ευρωσύστημα δυνάμει του κανονισμού ΣΣΣΠ θα πρέπει να διατυπώνονται με σαφήνεια στις αιτιολογικές σκέψεις του προτεινόμενου κανονισμού.

2.1.3 Στο ίδιο πνεύμα, η ΕΚΤ επικροτεί την εξαίρεση από την εφαρμογή του πλαισίου επίβλεψης που θεσπίζεται με τον προτεινόμενο κανονισμό των τρίτων παρόχων υπηρεσιών ΤΠΕ που υπόκεινται σε πλαίσια εποπτείας, τα οποία έχουν θεσπιστεί με σκοπό τη[ν] υποστήριξη των καθηκόντων που αναφέρονται στο άρθρο 127 παράγραφος 2 της Συνθήκης ([25]). Συναφώς, η ΕΚΤ υπογραμμίζει ότι δεν εμπίπτουν στο πεδίο εφαρμογής του προτεινόμενου κανονισμού οι κεντρικές τράπεζες του ΕΣΚΤ που ενεργούν υπό την ιδιότητά τους ως νομισματικών αρχών ([26]) και το Ευρωσύστημα όταν παρέχει υπηρεσίες μέσω του TARGET2, του TARGET2-Securities (T2S) ([27]) και του διακανονισμού άμεσων πληρωμών του TARGET (TIPS) ([28]), ούτε μπορούν να θεωρηθούν τρίτοι πάροχοι υπηρεσιών ΤΠΕ και, ως εκ τούτου, να χαρακτηριστούν ενδεχομένως ως κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ για τους σκοπούς του προτεινόμενου κανονισμού. Το Ευρωσύστημα ασκεί την επίβλεψη του T2S στο πλαίσιο της εξουσίας του για τη διασφάλιση αποτελεσματικών και υγιών συστημάτων συμψηφισμού και πληρωμών. Περαιτέρω, η ΕΑΚΑΑ έχει διευκρινίσει ότι το T2S δεν αποτελεί κρίσιμο πάροχο υπηρεσιών ([29]) κατά την έννοια του κανονισμού (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([30]) (εφεξής ο «κανονισμός για τα ΚΑΤ»). Συνεπώς, η οργανωτική και λειτουργική ασφάλεια, η αποδοτικότητα και η ανθεκτικότητα του T2S διασφαλίζονται μέσω του εφαρμοστέου νομικού, κανονιστικού και λειτουργικού πλαισίου και των συμφωνημένων ρυθμίσεων διακυβέρνησης ή του T2S, και όχι μέσω του κανονισμού για τα ΚΑΤ.

2.1.4 Επιπλέον, το πλαίσιο του Ευρωσυστήματος για την πολιτική επίβλεψης ([31]) καλύπτει κρίσιμους παρόχους υπηρεσιών, όπως η Society for Worldwide Interbank Financial Telecommunication (SWIFT). Η SWIFT είναι συνεταιριστική εταιρία περιορισμένης ευθύνης εγκατεστημένη στο Βέλγιο, η οποία παρέχει ασφαλείς υπηρεσίες αποστολής μηνυμάτων διεθνώς. Η Nationale Bank van België/Banque Nationale de Belgique ασκεί καθήκοντα ανώτατου οργάνου επίβλεψης της SWIFT και διενεργεί την επίβλεψη σε συνεργασία με τις λοιπές κεντρικές τράπεζες της Ομάδας των Δέκα (G10), περιλαμβανομένης της ΕΚΤ, βάσει σχετικών ρυθμίσεων από κοινού επίβλεψης. Τα όργανα επίβλεψης της Ομάδας των Δέκα (που) αναγνωρίζουν ότι επίκεντρο της επίβλεψης αποτελεί ο λειτουργικός κίνδυνος της SWIFT, καθώς αυτός θεωρείται η βασικότερη κατηγορία κινδύνου λόγω του οποίου αυτή θα μπορούσε να προκαλέσει συστημικό κίνδυνο στο χρηματοπιστωτικό σύστημα της Ένωσης. Στο πλαίσιο αυτό, η ομάδα από κοινού επίβλεψης της SWIFT (SWIFT Cooperative Oversight Group) κατάρτισε συγκεκριμένη δέσμη αρχών και απαιτήσεων υψηλού επιπέδου που έχουν εφαρμογή στη SWIFT, π.χ. εντοπισμός και διαχείριση κινδύνου, ασφάλεια πληροφοριών, αξιοπιστία και ανθεκτικότητα, προγραμματισμός τεχνολογίας και επικοινωνία με τους χρήστες. Τα όργανα επίβλεψης της Ομάδας των Δέκα (G10) ζητούν από τη SWIFT να προσχωρήσει στις ρυθμίσεις του εγγράφου της Επιτροπής Πληρωμών και Υποδομών της Αγοράς (CPMI) και του Διεθνούς Οργανισμού Επιτροπών Κινητών Αξιών (IOSCO) με τίτλο «Guidance on cyber resilience» («Οδηγίες για την κυβερνοανθεκτικότητα») ([32]), καθώς και σε άλλες διεθνείς προδιαγραφές ασφαλείας ΤΠΕ, οι οποίες, στο σύνολό τους, βαίνουν πέραν των απαιτήσεων του προτεινόμενου κανονισμού.

2.1.5 Κανείς δεν μπορεί να είναι βέβαιος ότι η SWIFT, και ενδεχομένως άλλοι πάροχοι υπηρεσιών που υπόκεινται στο πλαίσιο του Ευρωσυστήματος για την πολιτική επίβλεψης, θα μπορούσαν να εμπίπτουν στον προτεινόμενο κανονισμό ως τρίτοι πάροχοι υπηρεσιών ΤΠΕ στην περίπτωση παροχής υπηρεσιών που δεν καλύπτονται από το άρθρο 127 παράγραφος 2 της Συνθήκης. Ως εκ τούτου, η ΕΚΤ χαιρετίζει θερμά την εξαίρεση των παρόχων υπηρεσιών που υπόκεινται ήδη στο πλαίσιο του Ευρωσυστήματος για την πολιτική επίβλεψης, όπως, μεταξύ άλλων, της SWIFT, από το πεδίο εφαρμογής του πλαισίου επίβλεψης που θεσπίζεται με τον προτεινόμενο κανονισμό.

([25]) Βλέπε άρθρο 28 παράγραφος 5 του προτεινόμενου κανονισμού.

([26]) Βλέπε παράγραφο 1.3 της γνώμης της Ευρωπαϊκής Κεντρικής Τράπεζας, της 19ης Φεβρουαρίου 2021, σχετικά με πρόταση κανονισμού για τις αγορές κρυπτοστοιχείων και για την τροποποίηση της οδηγίας (ΕΕ) 2019/1937 (CON/2021/4). Όλες οι γνώμες της ΕΚΤ είναι δημοσιευμένες στο EUR-Lex.

([27]) Βλέπε παράρτημα IIα της κατευθυντήριας γραμμής ΕΚΤ/2012/27 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 5ης Δεκεμβρίου 2012, σχετικά με το Διευρωπαϊκό Αυτοματοποιημένο Σύστημα Ταχείας Μεταφοράς Κεφαλαίων και Διακανονισμού σε Συνεχή Χρόνο (TARGET2) (ΕΕ L 30 της 30.1.2013, σ. 1). Κατευθυντήρια γραμμή ΕΚΤ/2012/13 Ευρωπαϊκής Κεντρικής Τράπεζας, της 18ης Ιουλίου 2012, σχετικά με το TARGET2-Securities (ΕΕ L 215 της 11.8.2012, σ. 19)· απόφαση ΕΚΤ/2011/20 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 16ης Νοεμβρίου 2011, σχετικά με τη θέσπιση λεπτομερών κανόνων και διαδικασιών εφαρμογής των κριτηρίων επιλεξιμότητας όσον αφορά την πρόσβαση κεντρικών αποθετηρίων τίτλων στις υπηρεσίες του TARGET2-Securities (ΕΕ L 319 της 2.12.2011, σ. 117). Βλέπε επίσης τη συμφωνία-πλαίσιο για το T2S και τη συλλογική συμφωνία για το T2S.

([28]) Βλέπε παράρτημα IIβ της κατευθυντήριας γραμμής ΕΚΤ/2012/27.

([29]) Βλέπε άρθρο 30 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τη βελτίωση του διακανονισμού αξιογράφων στην Ευρωπαϊκή Ένωση και τα κεντρικά αποθετήρια τίτλων και για την τροποποίηση των οδηγιών 98/26/ΕΚ και 2014/65/ΕΕ και του κανονισμού (ΕΕ) αριθ. 236/2012 (ΕΕ L 257 της 28.8.2014, σ. 1) και άρθρο 68 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2017/392 της Επιτροπής, της 11ης Νοεμβρίου 2016, για τη συμπλήρωση του κανονισμού (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα για τις απαιτήσεις χορήγησης άδειας λειτουργίας και τις εποπτικές και λειτουργικές απαιτήσεις των κεντρικών αποθετηρίων τίτλων (ΕΕ L 65 της 10.3.2017, σ. 48).

([30]) Κανονισμός (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τη βελτίωση του διακανονισμού αξιογράφων στην Ευρωπαϊκή Ένωση και τα κεντρικά αποθετήρια τίτλων και για την τροποποίηση των οδηγιών 98/26/ΕΚ και 2014/65/ΕΕ και του κανονισμού (ΕΕ) αριθ. 236/2012 (ΕΕ L 257 της 28.8.2014, σ. 1).

([31]) «Eurosystem oversight policy framework», αναθεωρημένη έκδοση (Ιούλιος 2016), διαθέσιμη στον ιστότοπο της ΕΚΤ (www.ecb.europa.eu).

([32]) Διαθέσιμο στον ιστότοπο της Τράπεζας Διεθνών Διακανονισμών (www.bis.org).

2.2 *Καθήκοντα του ΕΣΚΤ στον τομέα του διακανονισμού αξιογράφων*

2.2.1 Τα κεντρικά αποθετήρια τίτλων (ΚΑΤ) αποτελούν υποδομές της χρηματοπιστωτικής αγοράς (FMI) οι οποίες ρυθμίζονται και εποπτεύονται αυστηρά από διαφορετικές αρχές βάσει του κανονισμού για τα ΚΑΤ, ο οποίος θεσπίζει απαιτήσεις διακανονισμού χρηματοπιστωτικών μέσων και κανόνες οργάνωσης και λειτουργίας των ΚΑΤ. Περαιτέρω, τα ΚΑΤ θα πρέπει να λαμβάνουν υπόψη το έγγραφο της CPMI-IOSCO με τίτλο «Guidance on cyber resilience» («Οδηγίες για την κυβερνοανθεκτικότητα»), για το οποίο έχουν δοθεί οδηγίες εφαρμογής στο έγγραφο με τίτλο «Cyber Resilience Oversight Expectations for financial market infrastructures» («Προσδοκίες επίβλεψης της κυβερνοανθεκτικότητας των υποδομών των χρηματοπιστωτικών αγορών») (Δεκέμβριος 2018) ([33]). Πέρα από τα εποπτικά καθήκοντα που ανατίθενται στις εθνικές αρμόδιες αρχές (ΕΑΑ) δυνάμει του κανονισμού για τα ΚΑΤ, τα μέλη του ΕΣΚΤ ενεργούν ως «οικείες αρχές», υπό την ιδιότητά τους ως εποπτικών αρχών των συστημάτων διακανονισμού αξιογράφων που τελούν υπό τη διαχείριση ΚΑΤ, ως κεντρικών τραπεζών που εκδίδουν τα πιο σημαντικά νομίσματα στα οποία πραγματοποιείται ο διακανονισμός και ως κεντρικών τραπεζών στα βιβλία των οποίων διακανονίζεται το χρηματικό σκέλος των συναλλαγών ([34]). Συναφώς, στην αιτιολογική σκέψη 8 του κανονισμού για τα ΚΑΤ αναφέρεται ότι οι διατάξεις του κανονισμού ισχύουν με την επιφύλαξη των αρμοδιοτήτων της ΕΚΤ και των εθνικών κεντρικών τραπεζών για τη διασφάλιση αποτελεσματικών και υγιών συστημάτων εκκαθάρισης και συστημάτων πληρωμών εντός της Ένωσης και σε άλλες χώρες. Στην αιτιολογική σκέψη 8 αναφέρεται επίσης ότι ο κανονισμός για τα ΚΑΤ δεν θα πρέπει να εμποδίζει την πρόσβαση των μελών του ΕΣΚΤ σε πληροφορίες σχετικές με την άσκηση των καθηκόντων τους ([35]), συμπεριλαμβανομένης της εποπτείας που ασκούν στα ΚΑΤ και σε άλλες FMI ([36]).

2.2.2 Επιπλέον, τα μέλη του ΕΣΚΤ ενεργούν συχνά ως διακανονιστές για το χρηματικό σκέλος των συναλλαγών αξιογράφων, ενώ το Ευρωσύστημα προσφέρει στα ΚΑΤ υπηρεσίες διακανονισμού μέσω του T2S. Η επίβλεψη του T2S από το Ευρωσύστημα συνδέεται με την εξουσία του τελευταίου να διασφαλίζει αποτελεσματικά και υγιή συστήματα συμψηφισμού και πληρωμών, ενώ οι αρμόδιες και οικείες αρχές των ΚΑΤ αποσκοπούν στην εξασφάλιση της ομαλής λειτουργίας τους, της ασφάλειας και αποτελεσματικότητας του διακανονισμού και της ορθής λειτουργίας των χρηματοπιστωτικών αγορών στις οικείες χώρες.

2.2.3 Βάσει του προτεινόμενου κανονισμού ([37]), οι κεντρικές τράπεζες του ΕΣΚΤ δεν μετέχουν στην κατάρτιση τεχνικών προτύπων για την εξειδίκευση των κινδύνων ΤΠΕ. Ομοίως, βάσει του προτεινόμενου κανονισμού ([38]), οι σχετικές αρχές δεν ενημερώνονται για τυχόν συμβάντα που σχετίζονται με τις ΤΠΕ. Η κεντρική τράπεζα του ΕΣΚΤ θα πρέπει να διατηρεί τον ίδιο βαθμό συμμετοχής με αυτόν που προβλέπεται επί του παρόντος στον κανονισμό για τα ΚΑΤ, ενώ οι σχετικές αρχές θα πρέπει να ενημερώνονται για τα συμβάντα που σχετίζονται με τις ΤΠΕ. Το Ευρωσύστημα είναι η αρμόδια αρχή για όλα τα ΚΑΤ της ζώνης του ευρώ και για ορισμένα άλλα ΚΑΤ της Ευρωπαϊκής Ένωσης. Οι κεντρικές τράπεζες του ΕΣΚΤ πρέπει να ενημερώνονται για τα συμβάντα που σχετίζονται με τις ΤΠΕ και είναι κρίσιμα για την άσκηση των καθηκόντων τους, συμπεριλαμβανομένης της εποπτείας που ασκούν στα ΚΑΤ και σε άλλες FMI. Οι κίνδυνοι στους οποίους εκτίθενται τα ΚΑΤ, συμπεριλαμβανομένων των κινδύνων ΤΠΕ, ενδέχεται να αποτελέσουν απειλή για την υγιή λειτουργία των ΚΑΤ. Ως εκ τούτου, οι κίνδυνοι ΤΠΕ είναι σημαντικοί για τις σχετικές αρχές, στις οποίες θα πρέπει να παρέχεται πλήρης και λεπτομερής επισκόπηση των εν λόγω κινδύνων προκειμένου να τους αξιολογούν και να επηρεάζουν την προσέγγιση της διαχείρισής τους από τα ΚΑΤ. Ο προτεινόμενος κανονισμός δεν θα πρέπει να θεσπίζει απαιτήσεις κινδύνων ΤΠΕ λιγότερο περιοριστικές από εκείνες του κανονισμού για τα ΚΑΤ και των συναφών ρυθμιστικών τεχνικών προτύπων που ήδη ισχύουν.

2.2.4 Επιπλέον, τα νομοθετικά όργανα της Ένωσης θα πρέπει να αποσαφηνίσουν την αλληλεπίδραση μεταξύ του προτεινόμενου κανονισμού ([39]) και των ρυθμιστικών τεχνικών προτύπων που συμπληρώνουν τον κανονισμό για τα ΚΑΤ. Ειδικότερα, δεν είναι σαφές εάν ορισμένο ΚΑΤ απαλλάσσεται από την υποχρέωση να διαθέτει τον δικό του δευτερεύοντα τόπο όταν ο τρίτος πάροχος υπηρεσιών ΤΠΕ του εν λόγω ΚΑΤ διατηρεί τέτοιο τόπο ([40]). Σε περίπτωση

([33]) Διαθέσιμο στον ιστότοπο της ΕΚΤ (www.ecb.europa.eu).

([34]) Βλέπε άρθρο 12 του κανονισμού (ΕΕ) αριθ. 909/2014.

([35]) Βλέπε επίσης άρθρο 13, άρθρο 17 παράγραφος 4 και άρθρο 22 παράγραφος 6 του κανονισμού (ΕΕ) αριθ. 909/2014.

([36]) Βλέπε παράγραφο 7.3 της γνώμης της Ευρωπαϊκής Κεντρικής Τράπεζας, της 6ης Απριλίου 2017, σχετικά με τον προσδιορισμό των κρίσιμων υποδομών προς τον σκοπό της ασφάλειας της τεχνολογίας πληροφοριών (CON/2017/10)· παράγραφο 7.2 της γνώμης της Ευρωπαϊκής Κεντρικής Τράπεζας, της 8ης Νοεμβρίου 2018, σχετικά με τον καθορισμό βασικών υπηρεσιών και διαχειριστών βασικών υπηρεσιών για τον σκοπό της ασφάλειας δικτύου και πληροφοριακών συστημάτων (CON/2018/47)· παράγραφο 3.5.2 της γνώμης της Ευρωπαϊκής Κεντρικής Τράπεζας, της 2ας Μαΐου 2019, σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών (CON/2019/17)· και παράγραφο 3.5.2 της γνώμης της Ευρωπαϊκής Κεντρικής Τράπεζας, της 11ης Νοεμβρίου 2019, σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών (CON/2019/38).

([37]) Βλέπε άρθρο 54 παράγραφος 5 του προτεινόμενου κανονισμού και άρθρο 45 παράγραφος 7 του κανονισμού (ΕΕ) αριθ. 909/2014.

([38]) Βλέπε άρθρο 54 παράγραφος 4 του προτεινόμενου κανονισμού και άρθρο 45 παράγραφος 6 του κανονισμού (ΕΕ) αριθ. 909/2014.

([39]) Βλέπε άρθρο 11 παράγραφος 5 του προτεινόμενου κανονισμού.

([40]) Βλέπε άρθρο 78 παράγραφος 3 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2017/392 της Επιτροπής, της 11ης Νοεμβρίου 2016, για τη συμπλήρωση του κανονισμού (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά τα ρυθμιστικά τεχνικά πρότυπα για τις απαιτήσεις χορήγησης άδειας λειτουργίας και τις εποπτικές και λειτουργικές απαιτήσεις των κεντρικών αποθετηρίων τίτλων (ΕΕ L 65 της 10.3.2017, σ. 48).

απαλλαγής ΚΑΤ από την εν λόγω υποχρέωση καθίσταται ασαφής η νομική ισχύς της. Στο ίδιο πνεύμα, ο προτεινόμενος κανονισμός ([41]) αναφέρεται σε στόχο που αφορά τον χρόνο αποκατάστασης και σε στόχους που αφορούν το σημείο αποκατάστασης για κάθε λειτουργία ([42]), ενώ το οικείο ρυθμιστικό τεχνικό πρότυπο διακρίνει μεταξύ κρίσιμων λειτουργιών (critical functions ([43]) και critical operations) ([44]) όσον αφορά τον χρόνο αποκατάστασης που ορίζεται για τις κρίσιμες λειτουργίες των ΚΑΤ. Η περαιτέρω αποσαφήνιση και εξέταση από τα νομοθετικά όργανα της Ένωσης δικαιολογείται από την αλληλεπίδραση μεταξύ του προτεινόμενου κανονισμού και των ρυθμιστικών τεχνικών προτύπων για τη συμπλήρωση του κανονισμού για τα ΚΑΤ προς αποτροπή του κινδύνου αντικρουόμενων απαιτήσεων. Τέλος, θα πρέπει να διευκρινιστεί ότι οι εξαιρέσεις που χορηγήθηκαν στα ΚΑΤ τα οποία τελούν υπό τη διαχείριση ορισμένων δημόσιων φορέων βάσει του κανονισμού για τα ΚΑΤ ([45]) παρατείνονται βάσει του προτεινόμενου κανονισμού.

2.3 *Καθήκοντα ΕΣΚΤ στον τομέα του συμψηφισμού αξιογράφων*

2.3.1 Οι κεντρικές τράπεζες του ΕΣΚΤ είναι επιφορτισμένες με καθήκοντα επίβλεψης των κεντρικών αντισυμβαλλομένων (ΚΑ). Συναφώς, οι εθνικές κεντρικές τράπεζες του Ευρωσυστήματος συνεργάζονται συχνά με τις οικείες εθνικές αρμόδιες αρχές σε σχέση με τα καθήκοντα επίβλεψης και εποπτείας που ασκούν στους ΚΑ και συμμετέχουν στο αντίστοιχο σώμα του ΚΑ που έχει συσταθεί βάσει του κανονισμού (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([46]) (εφεξής ο «EMIR»). Τα οικεία μέλη του Ευρωσυστήματος ([47]) συμμετέχουν στα σώματα του EMIR υπό την ιδιότητά τους ως αρχής που ασκεί την επίβλεψη και εκπροσωπούν το Ευρωσύστημα ως κεντρική τράπεζα έκδοσης για ΚΑ όταν το ευρώ είναι ένα από τα πιο σχετικά νομίσματα ως προς τα χρηματοπιστωτικά μέσα που συμψηφίζονται (και για εξωχώριους ΚΑ οι οποίοι συμψηφίζουν σημαντικό ποσοστό χρηματοπιστωτικών μέσων σε ευρώ). Η ΕΚΤ είναι η κεντρική τράπεζα έκδοσης για ΚΑ εκτός της ζώνης του ευρώ.

2.3.2 Βάσει του προτεινόμενου κανονισμού ([48]), οι κεντρικές τράπεζες του ΕΣΚΤ δεν μετέχουν στην κατάρτιση τεχνικών προτύπων για την εξειδίκευση των κινδύνων ΤΠΕ. Επιπλέον, από τον προτεινόμενο κανονισμό ([49]) απουσιάζει οποιαδήποτε αναφορά στις απαιτήσεις του EMIR σχετικά με τον στόχο που αφορά τον χρόνο αποκατάστασης και τον στόχο που αφορά το σημείο αποκατάστασης ([50]). Η προτεινόμενη ρυθμιστική πράξη δεν θα πρέπει να προβλέπει απαιτήσεις κινδύνων ΤΠΕ λιγότερο περιοριστικές από τις υφιστάμενες. Ως εκ τούτου, είναι κρίσιμο να τεθούν σαφείς στόχοι που αφορούν τον χρόνο και το σημείο αποκατάστασης προκειμένου να εξασφαλιστεί ένα υγιές πλαίσιο διαχείρισης αδιάλειπτης λειτουργίας. Η διατήρηση συγκεκριμένων στόχων που αφορούν τον χρόνο και το σημείο αποκατάστασης περιλαμβάνεται επίσης στο έγγραφο των CPMI-IOSCO με τίτλο «Principles for Financial Market Infrastructures» ([51]). Η ισχύουσα διάταξη του EMIR θα πρέπει να διατηρηθεί, και ο προτεινόμενος κανονισμός θα πρέπει να τροποποιηθεί αντίστοιχα. Οι κεντρικές τράπεζες του ΕΣΣΚ θα πρέπει να μετέχουν στην προπαρασκευή δευτερογενούς νομοθεσίας, καθώς και στην περαιτέρω αποσαφήνιση και εξέταση από τα νομοθετικά όργανα της Ένωσης της αλληλεπίδρασης μεταξύ του προτεινόμενου κανονισμού και των συμπληρωματικών ρυθμιστικών τεχνικών προτύπων προς αποτροπή του κινδύνου αντικρουόμενων ή αλληλοεπικαλυπτόμενων απαιτήσεων.

3. **Ειδικές παρατηρήσεις σχετικά με τις πτυχές προληπτικής εποπτείας**

3.1 Ο κανονισμός (ΕΕ) αριθ. 1024/2013 του Συμβουλίου ([52]) (εφεξής ο «κανονισμός ΕΕΜ») αναθέτει στην ΕΚΤ ειδικά καθήκοντα σχετικά με την προληπτική εποπτεία των πιστωτικών ιδρυμάτων εντός της ζώνης του ευρώ και την καθιστά υπεύθυνη για την αποτελεσματική και συνεπή λειτουργία του ενιαίου εποπτικού μηχανισμού (ΕΕΜ) στο πλαίσιο του οποίου κατανέμονται ειδικές εποπτικές αρμοδιότητες μεταξύ της ΕΚΤ και των συμμετεχουσών ΕΑΑ. Ειδικότερα, η ΕΚΤ είναι αρμόδια για τη χορήγηση και ανάκληση της άδειας λειτουργίας όλων των πιστωτικών ιδρυμάτων. Η ΕΚΤ είναι επίσης μεταξύ άλλων αρμόδια να διασφαλίζει τη συμμόρφωση με τη συναφή ενωσιακή νομοθεσία, θεσπίζοντας υποχρεώσεις προληπτικής εποπτείας για τα πιστωτικά ιδρύματα, συμπεριλαμβανομένης της υποχρέωσής τους να διαθέτουν άρτιες ρυθμίσεις διακυβέρνησης, όπως υγιείς διαδικασίες αξιολόγησης του κινδύνου και μηχανισμούς εσωτερικού ελέγχου ([53]). Προς τον σκοπό αυτό απονέμονται στην ΕΚΤ όλες οι εποπτικές εξουσίες παρέμβασης στη δραστηριότητα των πιστωτικών

([41]) Βλέπε άρθρο 11 παράγραφος 6 του προτεινόμενου κανονισμού.
([42]) Βλέπε άρθρο 3 παράγραφος 17 του προτεινόμενου κανονισμού.
([43]) Βλέπε άρθρο 76 παράγραφος 2 στοιχεία δ) και ε) του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2017/392 της Επιτροπής.
([44]) Βλέπε άρθρο 78 παράγραφοι 2 και 3 του κατ' εξουσιοδότηση κανονισμού (ΕΕ) 2017/392 της Επιτροπής.
([45]) Βλέπε άρθρο 1 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 909/2014.
([46]) Κανονισμός (ΕΕ) αριθ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2012, για τα εξωχρηματιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών (ΕΕ L 201, 27.7.2012, σ. 1).
([47]) Βλέπε άρθρο 18 παράγραφος 2 στοιχεία ζ) και η) του EMIR.
([48]) Βλέπε άρθρο 53 παράγραφος 2 στοιχείο β) και παράγραφος 3 του προτεινόμενου κανονισμού, καθώς και άρθρο 34 παράγραφος 3 του EMIR.
([49]) Βλέπε άρθρο 53 παράγραφος 2 στοιχείο α) του προτεινόμενου κανονισμού.
([50]) Βλέπε άρθρο 34 του EMIR.
([51]) Βλέπε έγγραφο των CPMI-IOSCO με τίτλο «Principles for Financial Market Infrastructures», το οποίο είναι διαθέσιμο στον ιστότοπο της Τράπεζας Διεθνών Διακανονισμών (www.bis.org).
([52]) Κανονισμός (ΕΕ) αριθ. 1024/2013 του Συμβουλίου, της 15ης Οκτωβρίου 2013 , για την ανάθεση ειδικών καθηκόντων στην Ευρωπαϊκή Κεντρική Τράπεζα σχετικά με τις πολιτικές που αφορούν την προληπτική εποπτεία των πιστωτικών ιδρυμάτων (ΕΕ L 287 της 29.10.2013, σ. 63).
([53]) Βλέπε άρθρο 4 παράγραφος 1 στοιχείο ε) και άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013.

ιδρυμάτων που είναι αναγκαίες για την άσκηση των καθηκόντων της. Ως εκ τούτου, η ΕΚΤ και οι οικείες ΕΑΑ είναι οι αρμόδιες αρχές για την άσκηση συγκεκριμένων εξουσιών προληπτικής εποπτείας δυνάμει του κανονισμού 2013/575/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([54]) (εφεξής ο «κανονισμός για τις κεφαλαιακές απαιτήσεις») και της οδηγίας 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([55]) (εφεξής η «οδηγία για τις κεφαλαιακές απαιτήσεις»).

3.2 Ο προτεινόμενος κανονισμός ορίζει ότι το ενιαίο εγχειρίδιο κανόνων και το σύστημα εποπτείας θα πρέπει να εξελιχθούν περαιτέρω ώστε να καλύπτουν την ψηφιακή επιχειρησιακή ανθεκτικότητα και την ασφάλεια ΤΠΕ με τη διεύρυνση των εντολών των αρχών χρηματοπιστωτικής εποπτείας που είναι επιφορτισμένες με καθήκοντα παρακολούθησης και προστασίας της χρηματοπιστωτικής σταθερότητας και της ακεραιότητας της αγοράς ([56]). Σκοπός είναι η ενίσχυση ενός ολοκληρωμένου πλαισίου για τους κινδύνους ΤΠΕ ή τους λειτουργικούς κινδύνους μέσω της εναρμόνισης των βασικών απαιτήσεων ψηφιακής επιχειρησιακής ανθεκτικότητας για όλες τις χρηματοπιστωτικές οντότητες ([57]). Ειδικότερα, με τον προτεινόμενο κανονισμό επιδιώκονται η ενοποίηση και η αναβάθμιση των απαιτήσεων σχετικά με τους κινδύνους ΤΠΕ, οι οποίες αντιμετωπίζονται μέχρι στιγμής χωριστά σε διαφορετικά νομοθετήματα της Ένωσης ([58]).

3.3 Οι απαιτήσεις σχετικά με τους κινδύνους ΤΠΕ για τον χρηματοπιστωτικό τομέα είναι διασκορπισμένες σε διάφορες πράξεις του δικαίου της Ένωσης, συμπεριλαμβανομένης της οδηγίας για τις κεφαλαιακές απαιτήσεις, και σε πράξεις ήπιου δικαίου (όπως οι κατευθυντήριες γραμμές της ΕΑΤ), είναι δε ανομοιογενείς και ενίοτε ελλιπείς. Σε ορισμένες περιπτώσεις, οι κίνδυνοι ΤΠΕ αντιμετωπίζονται μόνον εμμέσως, στο πλαίσιο του λειτουργικού κινδύνου, ενώ σε άλλες περιπτώσεις δεν αντιμετωπίζονται καθόλου. Τούτο θα πρέπει να επανορθωθεί με την ευθυγράμμιση του προτεινόμενου κανονισμού και των εν λόγω πράξεων. Προς τον σκοπό αυτό, η προτεινόμενη τροποποιητική οδηγία προκρίνει μια δέσμη τροποποιήσεων που φαίνονται απαραίτητες για την εξασφάλιση νομικής σαφήνειας και συνοχής σε σχέση με την εφαρμογή των διαφόρων απαιτήσεων ψηφιακής επιχειρησιακής ανθεκτικότητας. Πάντως, οι τροποποιήσεις της οδηγίας για τις κεφαλαιακές απαιτήσεις τις οποίες προτείνει επί του παρόντος η προτεινόμενη τροποποιητική οδηγία ([59]) αναφέρονται μόνον στις διατάξεις για σχέδια αντιμετώπισης επειγουσών καταστάσεων και συνέχισης της λειτουργίας ([60]), δοθέντος ότι υποτίθεται ότι χρησιμεύουν, εμμέσως, ως βάση για να καλυφθεί η διαχείριση των κινδύνων ΤΠΕ.

3.4 Περαιτέρω, ο προτεινόμενος κανονισμός ([61]) ορίζει ότι οι χρηματοπιστωτικές οντότητες, συμπεριλαμβανομένων των πιστωτικών ιδρυμάτων, εφαρμόζουν πλαίσια εσωτερικής διακυβέρνησης και ελέγχου τα οποία διασφαλίζουν την αποτελεσματική και συνετή διαχείριση όλων των κινδύνων ΤΠΕ. Ο προτεινόμενος κανονισμός ([62]) προβλέπει την εφαρμογή σε μεμονωμένο και ενοποιημένο επίπεδο των απαιτήσεων που θεσπίζει, αλλά χωρίς επαρκή συντονισμό με την τομεακή νομοθεσία στην οποία παραπέμπει. Τέλος, ο προτεινόμενος κανονισμός ([63]) προβλέπει ότι με την επιφύλαξη των διατάξεων σχετικά με το πλαίσιο επίβλεψης κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ που αναφέρονται στις διατάξεις του ([64]), η συμμόρφωση των πιστωτικών ιδρυμάτων με τις υποχρεώσεις που αυτός θεσπίζει διασφαλίζεται από την αρμόδια αρχή που ορίζεται σύμφωνα με το άρθρο 4 της οδηγίας για τις κεφαλαιακές απαιτήσεις, με την επιφύλαξη των ειδικών καθηκόντων που ανατίθενται στην ΕΚΤ δυνάμει του κανονισμού ΕΕΜ.

3.5 Λαμβανομένων υπόψη των παραπάνω, η ΕΚΤ αντιλαμβάνεται ότι, όσον αφορά τα πιστωτικά ιδρύματα, και εξαιρουμένων των διατάξεων του προτεινόμενου κανονισμού σχετικά με το πλαίσιο εποπτείας κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ ([65]), ο κανονισμός αυτός αποσκοπεί στη θέσπιση προληπτικού πλαισίου εσωτερικής διακυβέρνησης για τη διαχείριση των κινδύνων ΤΠΕ το οποίο θα ενσωματωθεί στο γενικό πλαίσιο εσωτερικής διακυβέρνησης βάσει της οδηγίας για τις κεφαλαιακές απαιτήσεις. Επιπλέον, δοθέντος του προληπτικού χαρακτήρα του προτεινόμενου πλαισίου, οι αρμόδιες αρχές για την εποπτεία της συμμόρφωσης με τις υποχρεώσεις που θεσπίζονται με το εν λόγω πλαίσιο, συμπεριλαμβανομένης της ΕΚΤ, θα είναι οι αρχές που είναι επιφορτισμένες με την τραπεζική εποπτεία σύμφωνα με τον κανονισμό ΕΕΜ.

([54]) Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και επιχειρήσεις επενδύσεων και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

([55]) Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, για την τροποποίηση της οδηγίας 2002/87/ΕΚ και για την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

([56]) Βλέπε αιτιολογική σκέψη 8 του προτεινόμενου κανονισμού.

([57]) Βλέπε αιτιολογική σκέψη 11 του προτεινόμενου κανονισμού.

([58]) Βλέπε αιτιολογική σκέψη 12 του προτεινόμενου κανονισμού.

([59]) Βλέπε αιτιολογικές σκέψεις 4 και 5 της προτεινόμενης τροποποιητικής οδηγίας.

([60]) Βλέπε άρθρο 85 της οδηγίας για τις κεφαλαιακές απαιτήσεις.

([61]) Βλέπε άρθρο 4 παράγραφος 1 του προτεινόμενου κανονισμού.

([62]) Βλέπε άρθρο 25 παράγραφοι 3 και 4 του προτεινόμενου κανονισμού.

([63]) Βλέπε άρθρο 41 του προτεινόμενου κανονισμού.

([64]) Βλέπε τμήμα ΙΙ του κεφαλαίου V του προτεινόμενου κανονισμού.

([65]) Βλέπε τμήμα ΙΙ του κεφαλαίου V του προτεινόμενου κανονισμού.

3.6 Τα νομοθετικά όργανα της Ένωσης θα μπορούσαν, ως εκ τούτου, να λάβουν υπόψη τις ακόλουθες προτάσεις για ενίσχυση της σαφήνειας και του συντονισμού μεταξύ του προτεινόμενου κανονισμού και της οδηγίας για τις κεφαλαιακές απαιτήσεις. Πρώτον, οι απαιτήσεις του προτεινόμενου κανονισμού μπορούν ρητά να χαρακτηριστούν ως εποπτικές, όπως συνέβη, μεταξύ άλλων, στον κανονισμό για τα ΚΑΤ ([66]). Δεύτερον, οι αιτιολογικές σκέψεις της προτεινόμενης τροποποιητικής οδηγίας ([67]) θα μπορούσαν να διατυπωθούν ευρύτερα, δεδομένου ότι οι απαιτήσεις του προτεινόμενου κανονισμού εκτείνονται πέραν της αμιγούς φάσης των σχεδίων αντιμετώπισης επειγουσών καταστάσεων και συνέχισης της λειτουργίας των επιχειρήσεων. Τα μέτρα διακυβέρνησης των κινδύνων ΤΠΕ συνολικά εμπίπτουν στο γενικότερο πεδίο των άρτιων ρυθμίσεων διακυβέρνησης βάσει του άρθρου 74 της οδηγίας για τις κεφαλαιακές απαιτήσεις ([68]). Τρίτον, ο προτεινόμενος κανονισμός ([69]) θα πρέπει να τροποποιηθεί, προκειμένου οι αιτιολογικές σκέψεις του να υπομιμνήσκουν την αρμοδιότητα της ΕΚΤ για την προληπτική εποπτεία πιστωτικών ιδρυμάτων βάσει της Συνθήκης και του κανονισμού ΕΕΜ. Τέταρτον, θα πρέπει να αναθεωρηθεί η αναφορά στην εφαρμογή σε μεμονωμένο και ενοποιημένο επίπεδο των απαιτήσεων που θεσπίζονται με αυτόν ([70]), δεδομένου ότι τα υποενοποιημένα και ενοποιημένα επίπεδα δεν ορίζονται στον προτεινόμενο κανονισμό και ορισμένοι τύποι διαμεσολαβητών δεν υπόκεινται σε ενοποιημένη εποπτεία βάσει της σχετικής νομοθεσίας (π.χ. ιδρύματα πληρωμών). Επιπλέον, το επίπεδο εφαρμογής των απαιτήσεων του προτεινόμενου κανονισμού θα πρέπει να πηγάζει αποκλειστικά από τη νομοθεσία που ισχύει για κάθε τύπο χρηματοπιστωτικής οντότητας. Στην περίπτωση των πιστωτικών ιδρυμάτων, προβλέπεται σαφής σύνδεση μεταξύ της οδηγίας για τις κεφαλαιακές απαιτήσεις και του προτεινόμενου κανονισμού, με αποτέλεσμα οι απαιτήσεις του προτεινόμενου κανονισμού να εφαρμόζονται αυτόματα σε μεμονωμένο, υποενοποιημένο ή ενοποιημένο επίπεδο ([71]), ανάλογα με την περίπτωση. Τέλος, τα νομοθετικά όργανα της Ένωσης θα μπορούσαν να εξετάσουν το ενδεχόμενο πρόβλεψης μεταβατικού καθεστώτος για τη διαχείριση της περιόδου μεταξύ της έναρξης ισχύος του προτεινόμενου κανονισμού και της έναρξης ισχύος των ρυθμιστικών τεχνικών προτύπων που προβλέπονται σε αυτόν, δεδομένου ότι ορισμένοι διαμεσολαβητές, συμπεριλαμβανομένων των πιστωτικών ιδρυμάτων, υπόκεινται ήδη σε κανόνες σχετικά με τους κινδύνους ΤΠΕ που εφαρμόζονται σε συγκεκριμένους τομείς και είναι λεπτομερέστεροι από τις γενικές διατάξεις του προτεινόμενου κανονισμού.

3.7 Η ΕΚΤ έχει επιφορτιστεί βάσει του κανονισμού ΕΕΜ με το καθήκον να διασφαλίζει τη συμμόρφωση των πιστωτικών ιδρυμάτων με τις απαιτήσεις της ενωσιακής νομοθεσίας βάσει της οποίας εκείνα πρέπει να διαθέτουν άρτιες διαδικασίες διαχείρισης κινδύνων και μηχανισμούς εσωτερικού ελέγχου ([72]). Αυτό σημαίνει ότι η ΕΚΤ πρέπει να διασφαλίζει ότι τα πιστωτικά ιδρύματα εφαρμόζουν πολιτικές και διαδικασίες για την αξιολόγηση και τη διαχείριση των ανοιγμάτων τους σε λειτουργικό κίνδυνο, συμπεριλαμβανομένων του κινδύνου υποδείγματος, και την κάλυψη γεγονότων με χαμηλή συχνότητα και σοβαρές επιπτώσεις. Τα πιστωτικά ιδρύματα καλούνται να διατυπώνουν με σαφήνεια τι συνιστά λειτουργικό κίνδυνο για τους σκοπούς των εν λόγω πολιτικών και διαδικασιών ([73]).

3.8 Τον Ιούλιο του 2017 το διοικητικό συμβούλιο της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ) ενέκρινε το SSM Cyber Incident Reporting Framework (Πλαίσιο αναφοράς κυβερνοσυμβάντων του ΕΕΜ· εφεξής το «Πλαίσιο»), βάσει σχεδίου πρότασης του εποπτικού συμβουλίου σύμφωνα με το άρθρο 26 παράγραφος 8 και το άρθρο 6 παράγραφος 2 του κανονισμού ΕΕΜ, καθώς και με το άρθρο 21 παράγραφος 1 του κανονισμού (ΕΕ) αριθ. 468/2014 της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ/2014/17) ([74]). Το Πλαίσιο συνίσταται σε δεσμευτικό αίτημα (μεμονωμένες αποφάσεις με αποδέκτες πιστωτικά ιδρύματα) για παροχή πληροφοριών και/ή υποβολή εκθέσεων βάσει του άρθρου 10 του κανονισμού ΕΕΜ ([75]). Ορισμένες χώρες έχουν ήδη εφαρμόσει διαδικασία αναφοράς συμβάντων επιβάλλοντας στα πιστωτικά ιδρύματα την υποχρέωση να αναφέρουν στις ΕΑΑ τους όλα τα σημαντικά κυβερνοσυμβάντα. Ορισμένες χώρες αναφέρουν όλα τα σημαντικά

([66]) Βλέπε τίτλο του κεφαλαίου ΙΙ, τμήμα 4, με τίτλο «Απαιτήσεις προληπτικής εποπτείας» του κανονισμού για τα ΚΑΤ.

([67]) Βλέπε αιτιολογική σκέψη 4 της προτεινόμενης τροποποιητικής οδηγίας.

([68]) Το άρθρο 85 της οδηγίας 2013/36/ΕΕ αποτελεί απλώς εξειδίκευση. Συναφώς, βλέπε επίσης σ. 4, 11 και 37 των κατευθυντήριων γραμμών της Ευρωπαϊκής Αρχής Τραπεζών σχετικά με τις ΤΠΕ και τη διαχείριση των κινδύνων ασφάλειας, της 29ης Νοεμβρίου 2019 (εφεξής οι «κατευθυντήριες γραμμές ΕΑΤ»), όπου η γενική νομική βάση θεμελιώνεται ρητά στο άρθρο 74 της οδηγίας 2013/36/ΕΕ.

([69]) Βλέπε άρθρο 41 παράγραφος 1 του προτεινόμενου κανονισμού.

([70]) Βλέπε άρθρο 25 παράγραφοι 3 και 4 του προτεινόμενου κανονισμού.

([71]) Βλέπε επίσης άρθρο 109 της οδηγίας για τις κεφαλαιακές απαιτήσεις.

([72]) Βλέπε άρθρο 4 παράγραφος 1 στοιχείο ε) του κανονισμού ΕΕΜ.

([73]) Βλέπε άρθρο 85 της οδηγίας για τις κεφαλαιακές απαιτήσεις.

([74]) Κανονισμός (ΕΕ) αριθ. 468/2014 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 16ης Απριλίου 2014, που θεσπίζει το πλαίσιο συνεργασίας μεταξύ της Ευρωπαϊκής Κεντρικής Τράπεζας, των εθνικών αρμόδιων αρχών και των εθνικών εντεταλμένων αρχών εντός του ενιαίου εποπτικού μηχανισμού (κανονισμός για το πλαίσιο ΕΕΜ) (ΕΚΤ/2014/17) (ΕΕ L 141 της 14.5.2014, σ. 1).

([75]) Συγκεκριμένα, ένα κυβερνοσυμβάν (διαπιστωμένη πιθανή παραβίαση —είτε κακόβουλη είτε τυχαία— της ασφάλειας των πληροφοριών) πρέπει να αναφέρεται στην ΕΚΤ εάν πληρούται τουλάχιστον μία από τις ακόλουθες προϋποθέσεις: 1) υφίσταται ενδεχόμενος οικονομικός αντίκτυπος 5 εκατ. ευρώ ή 0,1% του κεφαλαίου κοινών μετοχών της κατηγορίας 1 (CET1)· 2) το συμβάν αναφέρεται δημόσια ή προκαλεί βλάβη της φήμης· 3) το συμβάν κλιμακώθηκε στον επικεφαλής της πληροφορικής (CIO) πέραν της τακτικής υποβολής εκθέσεων· 4) η τράπεζα κοινοποίησε το συμβάν στη CERT/CSIRT, σε οργανισμό για την ασφάλεια ή στην αστυνομία· 5) έχουν κινηθεί διαδικασίες αποκατάστασης μετά από καταστροφή ή διαδικασίες αδιάλειπτης λειτουργίας ή έχει προβληθεί απαίτηση εξ ασφαλίσεως όσον αφορά την ασφάλεια στον κυβερνοχώρο· 6) υπήρξε παραβίαση νομικών ή κανονιστικών απαιτήσεων· ή 7) η τράπεζα χρησιμοποιεί εσωτερικά κριτήρια και εκτιμήσεις εμπειρογνωμόνων (συμπεριλαμβανομένου ενός δυνητικού συστημικού αντίκτυπου) και αποφασίζει να ενημερώσει την ΕΚΤ.

κυβερνοσυμβάντα στις ΕΑΑ τους. Στις χώρες αυτές, σημαντικά πιστωτικά ιδρύματα θα εξακολουθούν να αναφέρουν συμβάντα στις ΕΑΑ, οι οποίες στη συνέχεια θα τα διαβιβάζουν χωρίς αδικαιολόγητη καθυστέρηση στην ΕΚΤ για λογαριασμό των εποπτευόμενων οντοτήτων. Επομένως, οι ανωτέρω αποφάσεις έχουν ως αποδέκτες και αυτές τις εθνικές αρμόδιες αρχές με σκοπό τη διαβίβαση των εν λόγω πληροφοριών στην ΕΚΤ βάσει του Πλαισίου. Η ΕΚΤ στηρίζει την προσπάθεια των νομοθετικών οργάνων της Ένωσης για προώθηση της εναρμόνισης και του εξορθολογισμού, μεταξύ άλλων, όσον αφορά το σύνολο των κανόνων και των υποχρεώσεων που ισχύουν για τα πιστωτικά ιδρύματα σχετικά με την αναφορά συμβάντων. Στο πνεύμα αυτό, η ΕΚΤ είναι έτοιμη να τροποποιήσει (και ενδεχομένως να καταργήσει) το Πλαίσιο, εφόσον παραστεί ανάγκη, υπό το πρίσμα της ενδεχόμενης έγκρισης του προτεινόμενου κανονισμού.

4. **Ειδικές παρατηρήσεις σχετικά με τη διαχείριση κινδύνων ΤΠΕ, την αναφορά συμβάντων, τις δοκιμές επιχειρησιακής ανθεκτικότητας και τον κίνδυνο τρίτων παρόχων ΤΠΕ**

4.1 *Διαχείριση κινδύνων ΤΠΕ*

4.1.1 Η ΕΚΤ χαιρετίζει τη θέσπιση από τον προτεινόμενο κανονισμό ενός άρτιου και ολοκληρωμένου πλαισίου διαχείρισης κινδύνων ΤΠΕ το οποίο περιλαμβάνει το έγγραφο της CPMI-IOSCO με τίτλο «Guidance on cyber resilience» («Οδηγίες για την κυβερνοανθεκτικότητα») και ευθυγραμμίζεται στενά με τις βέλτιστες πρακτικές, συμπεριλαμβανομένου του εγγράφου του Ευρωσυστήματος με τίτλο «Cyber Resilience Oversight Expectations for FMI» («Προσδοκίες επίβλεψης της κυβερνοανθεκτικότητας των υποδομών των χρηματοπιστωτικών αγορών»).

4.1.2 Η ΕΚΤ υποστηρίζει την άποψη ότι οι χρηματοπιστωτικές οντότητες θα πρέπει να προβαίνουν σε αξιολόγηση κινδύνων έπειτα από κάθε «σημαντική αλλαγή» της υποδομής των συστημάτων δικτύου και πληροφοριών ([76]). Τούτου λεχθέντος, ο προτεινόμενος κανονισμός δεν περιέχει ορισμό της έννοιας «σημαντική αλλαγή», δημιουργώντας ανεπιθύμητο περιθώριο για αποκλίνουσες ερμηνείες από χρηματοπιστωτικές οντότητες που θα μπορούσαν τελικά να εμποδίσουν τους στόχους εναρμόνισης του προτεινόμενου κανονισμού. Για λόγους ασφάλειας δικαίου, τα νομοθετικά όργανα της Ένωσης δύνανται να εξετάσουν την εισαγωγή ορισμού της έννοιας «σημαντική αλλαγή» στον προτεινόμενο κανονισμό.

4.1.3 Η ΕΚΤ υποστηρίζει εν γένει την άποψη ότι οι χρηματοπιστωτικές οντότητες, πλην των πολύ μικρών επιχειρήσεων, υποβάλλουν στις αρμόδιες αρχές έκθεση όσον αφορά το σχετικό κόστος και τις ζημίες που προκλήθηκαν από τις διαταραχές των ΤΠΕ και τα συμβάντα που σχετίζονται με τις ΤΠΕ ([77]). Πάντως, προς διασφάλιση της συνολικής αποτελεσματικότητας του συστήματος και προς αποφυγή του ενδεχομένου να επιβαρυνθούν οι αρμόδιες αρχές και οι χρηματοπιστωτικές οντότητες με υπερβολικά μεγάλο αριθμό εκθέσεων, τα νομοθετικά όργανα της Ένωσης θα μπορούσαν να διερευνήσουν λυσιτελώς τη θέσπιση κατώτατων ορίων, ενδεχομένως ποσοτικής φύσης.

4.1.4 Η ΕΚΤ αναγνωρίζει τη δυνατότητα των χρηματοπιστωτικών οντοτήτων να αναθέτουν σε ενδοομιλικές ή εξωτερικές επιχειρήσεις τα καθήκοντα επαλήθευσης της συμμόρφωσης με τις απαιτήσεις διαχείρισης κινδύνων ΤΠΕ, κατόπιν έγκρισης από τις αρμόδιες αρχές ([78]). Ταυτόχρονα, είναι σημαντικό τα νομοθετικά όργανα της Ένωσης να αποσαφηνίσουν τους όρους χορήγησης της εν λόγω έγκρισης σε περιπτώσεις στις οποίες ορισμένη χρηματοπιστωτική οντότητα υπόκειται σε πλείονες αρμόδιες αρχές. Αυτό θα μπορούσε να συμβεί όταν η χρηματοπιστωτική οντότητα είναι πιστωτικό ίδρυμα, πάροχος υπηρεσιών κρυπτοστοιχείων και/ή πάροχος υπηρεσιών πληρωμών. Τέλος, ως προς τον προσδιορισμό και την ταξινόμηση των περιουσιακών στοιχείων από τις χρηματοπιστωτικές οντότητες βάσει του προτεινόμενου κανονισμού ([79]), η ΕΚΤ θα έκρινε συνετό οι διατάξεις του να απαιτούν επίσης από τις οντότητες αυτές να λαμβάνουν υπόψη την κρισιμότητα των περιουσιακών αυτών στοιχείων για τους σκοπούς της ταξινόμησης (δηλαδή εάν αυτά υποστηρίζουν κρίσιμες λειτουργίες).

4.2 *Αναφορά συμβάντων*

4.2.1 Η ΕΚΤ χαιρετίζει τις προσπάθειες που σκιαγραφούνται στον προτεινόμενο κανονισμό για την εναρμόνιση του τοπίου αναφοράς συμβάντων που σχετίζονται με τις ΤΠΕ εντός της Ένωσης και τις εργασίες με σκοπό την κεντρική διαχείριση της αναφοράς σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ ([80]). Η θέσπιση εναρμονισμένου πλαισίου για την αναφορά σημαντικών συμβάντων που σχετίζονται με τις ΤΠΕ ([81]) στις οικείες αρμόδιες αρχές καταρχάς θα εξορθολογήσει και θα εναρμονίσει την επιβάρυνση των χρηματοπιστωτικών οντοτήτων —συμπεριλαμβανομένων των πιστωτικών ιδρυμάτων— σχετικά με την υποβολή αναφορών. Οι αρμόδιες αρχές θα επωφεληθούν από το μεγαλύτερο εύρος των καλυπτόμενων συμβάντων, βαίνοντας πέραν των συμβάντων τα οποία σχετίζονται με τον κυβερνοχώρο και καλύπτονται επί του παρόντος από τα υφιστάμενα πλαίσια ([82]). Η μελλοντική έγκριση του προτεινόμενου κανονισμού θα απαιτήσει αναθεώρηση και ενδεχομένως κατάργηση των υφιστάμενων πλαισίων, συμπεριλαμβανομένου του SSM Cyber Incident Reporting Framework (Πλαισίου αναφοράς κυβερνοσυμβάντων του ΕΕΜ). Τούτου λεχθέντος, προκειμένου να επιτευχθεί πραγματικός εξορθολογισμός και πλήρης ευθυγράμμιση όλων των πλαισίων, είναι κρίσιμο να διασφαλιστεί ότι το πεδίο

([76]) Βλέπε άρθρο 7 παράγραφος 3 του προτεινόμενου κανονισμού.
([77]) Βλέπε άρθρο 10 παράγραφος 9 του προτεινόμενου κανονισμού.
([78]) Βλέπε άρθρο 5 παράγραφος 10 του προτεινόμενου κανονισμού.
([79]) Βλέπε άρθρο 7 του προτεινόμενου κανονισμού.
([80]) Βλέπε άρθρο 19 του προτεινόμενου κανονισμού.
([81]) Βλέπε άρθρο 3 παράγραφος 7, καθώς και άρθρα 17 και 18 του προτεινόμενου κανονισμού.
([82]) Βλέπε, για παράδειγμα, το Πλαίσιο.

εφαρμογής των διατάξεων για την αναφορά συμβάντων βάσει του προτεινόμενου κανονισμού, συμπεριλαμβανομένων όλων των σχετικών ορισμών, των κατώτατων ορίων και των παραμέτρων αναφοράς, είναι πλήρως ευθυγραμμισμένο με τα οικεία πλαίσια. Ειδικότερα, είναι ύψιστης σημασίας να διασφαλιστεί η ευθυγράμμιση μεταξύ, αφενός, του προτεινόμενου κανονισμού, και, αφετέρου, της οδηγίας (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([83]) (εφεξής η «PSD2») και των κατευθυντήριων γραμμών της ΕΑΤ για την αναφορά μειζόνων συμβάντων (εφεξής οι «κατευθυντήριες γραμμές της ΕΑΤ»). Η προτεινόμενη τροποποιητική οδηγία ([84]) περιέχει τροποποιήσεις της PSD2 όσον αφορά την οριοθέτηση της αναφοράς συμβάντων μεταξύ του προτεινόμενου κανονισμού και της PSD2, οι οποίες θα επηρεάσουν κυρίως τους παρόχους υπηρεσιών πληρωμών, οι οποίοι θα μπορούσαν επίσης να αδειοδοτούνται ως πιστωτικά ιδρύματα, καθώς και τις αρμόδιες αρχές. Υφίσταται έλλειψη σαφήνειας όσον αφορά τη διαδικασία κοινοποίησης συμβάντων, καθώς και ενδεχόμενη αλληλοεπικάλυψη μεταξύ ορισμένων εκ των συμβάντων τα οποία πρέπει να αναφέρονται τόσο βάσει του προτεινόμενου κανονισμού όσο και βάσει των κατευθυντήριων γραμμών της ΕΑΤ.

4.2.2 Οι διαδικασίες για την κοινοποίηση σημαντικών συμβάντων, βάσει, αντίστοιχα, του προτεινόμενου κανονισμού ([85]), της PSD2 και των αντίστοιχων κατευθυντήριων γραμμών της ΕΑΤ θα απαιτούσαν από τους παρόχους υπηρεσιών πληρωμών την υποβολή αναφοράς συμβάντος στην αντίστοιχη αρμόδια αρχή μετά την ταξινόμηση του συμβάντος. Στην πραγματικότητα, οι αρχικές εκθέσεις δεν αποτυπώνουν την ουσία, τα αίτια ή τον λειτουργικό τομέα που επηρεάζεται από το συμβάν, ενώ οι πάροχοι υπηρεσιών πληρωμών ενδέχεται να είναι σε θέση να προβούν σε τέτοιου είδους διακρίσεις αποκλειστικά σε μεταγενέστερο στάδιο, όταν καταστούν διαθέσιμες λεπτομερέστερες πληροφορίες για το συμβάν. Συνεπώς, οι αρχικές εκθέσεις συμβάντων θα μπορούσαν να υποβληθούν τόσο βάσει του προτεινόμενου κανονισμού όσο και των κατευθυντήριων γραμμών της ΕΑΤ, ή, διαφορετικά, οι πάροχοι υπηρεσιών πληρωμών μπορούν να επιλέξουν ένα ενιαίο πλαίσιο αναφοράς συμβάντων και να διορθώσουν τις υποβληθείσες εκθέσεις τους σε μεταγενέστερη ημερομηνία. Η ίδια αβεβαιότητα (όσον αφορά, για παράδειγμα, τα βασικά αίτια οποιουδήποτε συμβάντος) μπορεί επίσης να αντικατοπτρίζεται στις ενδιάμεσες και τελικές εκθέσεις. Τούτο αυξάνει εκ νέου τη δυνατότητα παράλληλης υποβολής εκθέσεων στις αρμόδιες αρχές βάσει του προτεινόμενου κανονισμού και της PSD2.

4.2.3 Ορισμένα συμβάντα τα οποία ενδέχεται να ταξινομούνται ως συμβάντα που σχετίζονται με τις ΤΠΕ, μπορεί επίσης να έχουν επιπτώσεις σε άλλους τομείς και, ως εκ τούτου, θα πρέπει να κοινοποιούνται βάσει των κατευθυντήριων γραμμών της ΕΑΤ. Αυτό μπορεί να συμβαίνει όταν ένα συμβάν έχει επιπτώσεις από πλευράς ΤΠΕ, αλλά, ταυτόχρονα, έχει επηρεάσει και την παροχή υπηρεσιών πληρωμών άμεσα και/ή άλλους λειτουργικούς τομείς ή διαύλους εκτός τομέα ΤΠΕ. Επιπλέον, θα μπορούσαν να υπάρχουν περιπτώσεις όπου δεν είναι δυνατή η διάκριση μεταξύ συμβάντων που αφορούν τη λειτουργία και συμβάντων που σχετίζονται με τις ΤΠΕ. Περαιτέρω, στην περίπτωση που η ίδια χρηματοπιστωτική οντότητα είναι σημαντικό πιστωτικό ίδρυμα και πάροχος υπηρεσιών πληρωμών, σύμφωνα με τον προτεινόμενο κανονισμό, η ίδια οντότητα θα πρέπει να αναφέρει το συμβάν που σχετίζεται με τις ΤΠΕ δύο φορές, καθόσον υπόκειται σε δύο αρμόδιες αρχές. Λαμβανομένων υπόψη των προεκτεθέντων, ο προτεινόμενος κανονισμός θα πρέπει να διατυπώνει σαφέστερα τον τρόπο με τον οποίο η αλληλεπίδραση μεταξύ της PSD2 και των κατευθυντήριων γραμμών της ΕΒΑ πρόκειται να λειτουργήσει στην πράξη. Ιδίως δε, θα ήταν σημαντικό, για λόγους εναρμόνισης και εξορθολογισμού των υποχρεώσεων υποβολής εκθέσεων, τα νομοθετικά όργανα της Ένωσης να εξετάσουν εναπομένοντα ζητήματα διπλής υποβολής εκθέσεων και να αποσαφηνίσουν εάν ο προτεινόμενος κανονισμός, αφενός, και η PSD2 και οι κατευθυντήριες γραμμές της ΕΑΤ, αφετέρου, θα συνυπάρξουν ή εάν θα πρέπει να υπάρξει ενιαίο σύνολο απαιτήσεων αναφοράς συμβάντων.

4.2.4. Ο προτεινόμενος κανονισμός θεσπίζει την υποχρέωση σε βάρος των αρμόδιων αρχών ([86]), με την παραλαβή αναφοράς, να επιβεβαιώνουν την παραλαβή της κοινοποίησης και να παρέχουν το συντομότερο δυνατόν στη χρηματοπιστωτική οντότητα όλα τα απαραίτητα σχόλια και παρατηρήσεις ή καθοδήγηση, ιδίως για να συζητηθούν διορθωτικά μέτρα στο επίπεδο της οντότητας ή τρόποι για την ελαχιστοποίηση των αρνητικών επιπτώσεων στους διάφορους τομείς. Αυτό σημαίνει ότι οι αρμόδιες αρχές θα πρέπει να συμβάλουν ενεργά στη διαχείριση και την επανόρθωση συμβάντων, ενώ ταυτόχρονα θα αξιολογούν επίσης την ανταπόκριση μιας εποπτευόμενης οντότητας σε κρίσιμα συμβάντα. Η ΕΚΤ τονίζει ότι την ευθύνη της αποκατάστασης, καθώς και τις συνέπειες ενός συμβάντος θα πρέπει να εξακολουθεί να φέρει αποκλειστικώς και σαφώς η οικεία χρηματοπιστωτική οντότητα. Ως εκ τούτου, η ΕΚΤ προτείνει να περιοριστούν τα σχόλια και οι παρατηρήσεις, καθώς και η καθοδήγηση, αποκλειστικά σε σχόλια και παρατηρήσεις, καθώς και σε καθοδήγηση υψηλού επιπέδου σχετικά με την προληπτική εποπτεία. Εάν τα σχόλια και οι παρατηρήσεις ήταν ευρύτερα, θα απαιτούνταν εξειδικευμένοι επαγγελματίες με πολύ σημαντικές τεχνικές γνώσεις τις οποίες συνήθως δεν διαθέτει η δεξαμενή ταλέντου που έχουν στη διάθεσή τους οι αρχές προληπτικής εποπτείας.

4.3 *Δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας*

4.3.1 Η ΕΚΤ χαιρετίζει τις απαιτήσεις που θεσπίζονται με τον προτεινόμενο κανονισμό ([87]) σχετικά με τις δοκιμές ψηφιακής επιχειρησιακής ανθεκτικότητας στις χρηματοπιστωτικές οντότητες και την ανάγκη κάθε ιδρύματος να έχει το δικό του πρόγραμμα δοκιμών. Ο προτεινόμενος κανονισμός ([88]) περιγράφει ενδεικτικώς διάφορους τύπους δοκιμών για τις

([83]) Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35).
([84]) Βλέπε άρθρο 7 παράγραφος 9 της προτεινόμενης τροποποιητικής οδηγίας.
([85]) Βλέπε άρθρο 17 παράγραφος 3 του προτεινόμενου κανονισμού.
([86]) Βλέπε άρθρο 20 του προτεινόμενου κανονισμού.
([87]) Βλέπε άρθρα 21 και 22 του προτεινόμενου κανονισμού.
([88]) Βλέπε άρθρο 22 παράγραφος 1 του προτεινόμενου κανονισμού.

χρηματοπιστωτικές οντότητες. Οι τύποι των δοκιμών δεν είναι πολύ σαφείς, ενώ ορισμένες δοκιμές, όπως οι δοκιμές συμβατότητας, τα ερωτηματολόγια ή οι δοκιμές βάσει σεναρίων, επιδέχονται διαφορετικές ερμηνείες από τις ΕΕΑ, τις αρμόδιες αρχές ή τις χρηματοπιστωτικές οντότητες. Επιπλέον, δεν υπάρχουν επίσης οδηγίες ως προς τη συχνότητα κάθε δοκιμής. Μια πιθανή προσέγγιση θα μπορούσε να είναι η θέσπιση με τον προτεινόμενο κανονισμό γενικών απαιτήσεων δοκιμών, με ακριβέστερη περιγραφή των τύπων δοκιμών που καθορίζονται στα ρυθμιστικά και εκτελεστικά τεχνικά πρότυπα.

4.3.2 Οι δοκιμές διείσδυσης βάσει απειλών είναι ένα ισχυρό εργαλείο για τον έλεγχο της άμυνας και της ετοιμότητας στον τομέα της ασφάλειας. Ως εκ τούτου, η ΕΚΤ ενθαρρύνει τη διεξαγωγή δοκιμών διείσδυσης βάσει απειλών από χρηματοπιστωτικές οντότητες. Με αυτό το εργαλείο δεν υποβάλλονται σε δοκιμές μόνο τα τεχνικά μέτρα, αλλά και το προσωπικό και οι διαδικασίες. Τα αποτελέσματα των εν λόγω δοκιμών μπορούν να αυξήσουν σημαντικά την ευαισθητοποίηση των ανώτερων διοικητικών στελεχών σε θέματα ασφάλειας στις οντότητες που υποβάλλονται σε δοκιμές. Το ευρωπαϊκό πλαίσιο «Threat Intelligence Based Ethical Red-teaming (TIBER-EU)» ([89]) και άλλα εργαλεία δοκιμών διείσδυσης βάσει απειλών τα οποία είναι ήδη διαθέσιμα εκτός της Ένωσης, αποτελούν βασικά εργαλεία για την αξιολόγηση, τον έλεγχο, την προετοιμασία και τη βελτίωση, εκ μέρους των ίδιων των οντοτήτων, της θέσης και της άμυνάς τους όσον αφορά την κυβερνοανθεκτικότητα.

4.3.3 Στα περισσότερα κράτη μέλη όπου έχει εφαρμοστεί το TIBER-EU, οι αρχές επίβλεψης και οι αρχές εποπτείας δεν διαδραματίζουν ενεργό ρόλο στην εφαρμογή ενός τοπικού προγράμματος TIBER-XX και η ομάδα Cyber Team TIBER (TCT) ενεργεί σχεδόν σε όλες τις περιπτώσεις ανεξάρτητα από αυτές τις λειτουργίες. Για τον λόγο αυτό, οι προηγμένες δοκιμές βάσει του προτεινόμενου κανονισμού ([90]), μέσω δοκιμών διείσδυσης βάσει απειλών, θα πρέπει να χρησιμοποιούνται ως εργαλείο για την ενίσχυση του χρηματοπιστωτικού οικοσυστήματος, καθώς και για την ενίσχυση της χρηματοπιστωτικής σταθερότητας, και όχι ως αμιγώς εποπτικό εργαλείο. Επιπλέον, δεν απαιτείται η ανάπτυξη ενός νέου πλαισίου προηγμένων δοκιμών κυβερνοανθεκτικότητας, καθώς τα κράτη μέλη έχουν ήδη υιοθετήσει ευρέως το TIBER-EU, το οποίο είναι μοναδικό πλαίσιο αυτού του είδους στην Ευρωπαϊκή Ένωση επί του παρόντος.

4.3.4 Οι απαιτήσεις για τους φορείς δοκιμών δεν θα πρέπει να περιλαμβάνονται στις διατάξεις του προτεινόμενου κανονισμού, καθώς ο τομέας που σχετίζεται με δοκιμές διείσδυσης βάσει απειλών εξακολουθεί να αναπτύσσεται και η καινοτομία μπορεί να παρεμποδιστεί από την επιβολή ειδικών απαιτήσεων. Τούτου λεχθέντος, η ΕΚΤ είναι της άποψης ότι για να διασφαλιστεί υψηλός βαθμός ανεξαρτησίας κατά τη διεξαγωγή δοκιμών, οι χρηματοπιστωτικές οντότητες δεν θα πρέπει να απασχολούν ή να συνάπτουν συμβάσεις με φορείς δοκιμών οι οποίοι απασχολούνται ή έχουν συνάψει συμβάσεις με χρηματοπιστωτικές οντότητες στον δικό τους όμιλο ή οι οποίοι, υπό άλλους όρους, ανήκουν και/ή ελέγχονται από τις χρηματοπιστωτικές οντότητες που πρόκειται να υποβληθούν σε δοκιμές.

4.3.5 Προκειμένου να μειωθεί ο κίνδυνος κατακερματισμού και να διασφαλιστεί η εναρμόνιση, ο προτεινόμενος κανονισμός θα πρέπει να επιβάλει ένα πλαίσιο δοκιμών διείσδυσης βάσει απειλών το οποίο θα ισχύει για τον χρηματοπιστωτικό τομέα σε ολόκληρη την Ένωση. Ο κατακερματισμός μπορεί να οδηγήσει σε αύξηση του κόστους και των τεχνικών και λειτουργικών απαιτήσεων, καθώς και των απαιτήσεων για χρηματοοικονομικούς πόρους, τόσο για τις αρμόδιες αρχές όσο και για τα χρηματοπιστωτικά ιδρύματα. Το αυξημένο κόστος και οι αυξημένες απαιτήσεις ενδέχεται τελικά να έχουν αρνητικό αντίκτυπο στην αμοιβαία αναγνώριση των δοκιμών. Η εν λόγω έλλειψη εναρμόνισης και τα ανακύπτοντα ζητήματα αμοιβαίας αναγνώρισης είναι ιδιαίτερα κρίσιμα για τις χρηματοπιστωτικές οντότητες, οι οποίες ενδέχεται να διαθέτουν πολλαπλές άδειες και/ή να λειτουργούν σε πολλές χώρες σε ολόκληρη την Ένωση. Τα ρυθμιστικά και εκτελεστικά τεχνικά πρότυπα τα οποία πρόκειται να καταρτιστούν, βάσει του προτεινόμενου κανονισμού, σχετικά με τις δοκιμές διείσδυσης βάσει απειλών, θα πρέπει να είναι σύμφωνα με το TIBER-EU. Περαιτέρω, η ΕΚΤ χαιρετίζει την ευκαιρία να μετάσχει στην προετοιμασία των εν λόγω ρυθμιστικών και εκτελεστικών τεχνικών προτύπων σε συνεργασία με τις ΕΕΑ.

4.3.6 Η ενεργός συμμετοχή των αρμόδιων αρχών στις δοκιμές θα μπορούσε να οδηγήσει σε ενδεχόμενη σύγκρουση συμφερόντων με την άλλη λειτουργία που επιτελούν, δηλαδή την αξιολόγηση του πλαισίου δοκιμών της χρηματοπιστωτικής οντότητας. Στο πλαίσιο αυτό, η ΕΚΤ προτείνει να απαλειφθεί από τον προτεινόμενο κανονισμό κάθε υποχρέωση των αρμόδιων αρχών σχετικά με την επικύρωση εγγράφων και τη χορήγηση βεβαίωσης δοκιμής διείσδυσης βάσει απειλών.

4.4 Κίνδυνος τρίτων παρόχων ΤΠΕ

4.4.1 1 Η ΕΚΤ χαιρετίζει τη θέσπιση ενός ολοκληρωμένου συνόλου βασικών αρχών και ενός ισχυρού πλαισίου εποπτείας για τον εντοπισμό και τη διαχείριση των κινδύνων ΤΠΕ που προέρχονται από τρίτους παρόχους υπηρεσιών ΤΠΕ, ανεξαρτήτως του εάν ανήκουν στον ίδιο όμιλο χρηματοπιστωτικών οντοτήτων. Τούτου λεχθέντος, προκειμένου να επιτευχθεί αποτελεσματικός εντοπισμός και διαχείριση κινδύνων ΤΠΕ, είναι σημαντικό να εντοπίζονται και να ταξινομούνται ορθά, μεταξύ άλλων, κρίσιμοι τρίτοι πάροχοι υπηρεσιών ΤΠΕ. Συναφώς, μολονότι η θέσπιση κατ' εξουσιοδότηση πράξεων ([91]) οι οποίες θα συμπληρώνουν τα κριτήρια που πρόκειται να χρησιμοποιηθούν για σκοπούς ταξινόμησης ([92]) είναι ευπρόσδεκτη, εντούτοις, θα πρέπει να ζητείται η γνώμη της ΕΚΤ πριν από την έκδοση των εν λόγω πράξεων.

([89]) Διαθέσιμο στον ιστότοπο της ΕΚΤ (www.ecb.europa.eu).
([90]) Άρθρα 23 και 24 του προτεινόμενου κανονισμού.
([91]) Βλέπε άρθρο 28 παράγραφος 3 του προτεινόμενου κανονισμού.
([92]) Βλέπε άρθρο 28 παράγραφος 2 του προτεινόμενου κανονισμού.

4.4.2 Όσον αφορά τη δομή του πλαισίου εποπτείας ([93]), απαιτείται περαιτέρω αποσαφήνιση όσον αφορά τον ρόλο που θα αναλάβει η μεικτή επιτροπή. Ταυτόχρονα, η ΕΚΤ χαιρετίζει τη συμμετοχή της στο φόρουμ εποπτείας ως παρατηρητή, καθώς με τον εν λόγω ρόλο η ΕΚΤ θα αποκτήσει την ίδια πρόσβαση σε έγγραφα και πληροφορίες όπως τα μέλη με δικαίωμα ψήφου ([94]). Η ΕΚΤ θα ήθελε να επιστήσει την προσοχή των νομοθετικών οργάνων της Ένωσης στο γεγονός ότι η ίδια, στο ρόλο της ως παρατηρητή, θα συμβάλει στο έργο του φόρουμ εποπτείας, τόσο υπό την ιδιότητά της ως κεντρικής τράπεζας έκδοσης, η οποία είναι αρμόδια για την εποπτεία των υποδομών της αγοράς, όσο και υπό την ιδιότητά της ως αρχής προληπτικής εποπτείας των πιστωτικών ιδρυμάτων. Επιπλέον, η ΕΚΤ σημειώνει ότι η ίδια, εκτός από παρατηρητής στο φόρουμ εποπτείας, συμμετέχει επίσης, ως αρμόδια αρχή, στην κοινή εξεταστική ομάδα. Στο πλαίσιο αυτό, τα νομοθετικά όργανα της Ένωσης θα μπορούσαν να εξετάσουν περαιτέρω τη σύνθεση των κοινών εξεταστικών ομάδων ([95]) με σκοπό την εξασφάλιση δέουσας σημαντικής συμμετοχής των οικείων αρμόδιων αρχών. Στο ίδιο πνεύμα, η ΕΚΤ πιστεύει ότι ο μέγιστος αριθμός συμμετεχόντων στις κοινές εξεταστικές ομάδες θα πρέπει να αυξηθεί, λαμβανομένων υπόψη της κρισιμότητας, της πολυπλοκότητας και του εύρους των υπηρεσιών ΤΠΕ τρίτων.

4.4.3 Η ΕΚΤ σημειώνει ότι σύμφωνα με τον προτεινόμενο κανονισμό, ο κύριος εποπτικός φορέας μπορεί να αποτρέπει κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ από τη σύναψη περαιτέρω ρυθμίσεων υπεργολαβίας, εφόσον i) ο προβλεπόμενος υπεργολάβος είναι τρίτος πάροχος υπηρεσιών ΤΠΕ ή υπεργολάβος ΤΠΕ εγκατεστημένος σε τρίτη χώρα και ii) η υπεργολαβία αφορά κρίσιμη ή σημαντική λειτουργία της χρηματοπιστωτικής οντότητας. Η ΕΚΤ επιθυμεί να τονίσει ότι αυτές οι εξουσίες μπορούν να ασκούνται μόνον από τον κύριο εποπτικό φορέα στο πλαίσιο ρυθμίσεων υπεργολαβίας όταν ένας κρίσιμος πάροχος υπηρεσιών ΤΠΕ αναθέτει υπό μορφή υπεργολαβίας κρίσιμη ή σημαντική λειτουργία σε ξεχωριστή νομική οντότητα εγκατεστημένη σε τρίτη χώρα. Η ΕΚΤ αντιλαμβάνεται ότι ο κύριος εποπτικός φορέας δεν θα μπορούσε να ασκήσει ανάλογες εξουσίες για να αποτρέψει έναν κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ από την εξωτερική ανάθεση κρίσιμων ή σημαντικών λειτουργιών της χρηματοπιστωτικής οντότητας σε εγκαταστάσεις του παρόχου υπηρεσιών ευρισκόμενες σε τρίτη χώρα. Αυτό θα μπορούσε να συμβεί, για παράδειγμα, όταν, από επιχειρησιακής πλευράς, εγκαταστάσεις ευρισκόμενες εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ) αποθηκεύουν ή επεξεργάζονται κρίσιμα δεδομένα και/ή πληροφορίες. Σε μια τέτοια περίπτωση, ο κύριος εποπτικός φορέας ενδεχομένως να μην εξουσιοδοτεί επαρκώς τις αρμόδιες αρχές να έχουν πρόσβαση στο σύνολο των πληροφοριών, των χώρων, των υποδομών και του προσωπικού που σχετίζονται με την εκτέλεση όλων των κρίσιμων ή σημαντικών λειτουργιών της χρηματοπιστωτικής οντότητας. Προκειμένου να διασφαλιστεί η δυνατότητα των αρμόδιων αρχών να εκτελούν απρόσκοπτα τα καθήκοντά τους, η ΕΚΤ προτείνει να χορηγηθεί στον κύριο εποπτικό φορέα η εξουσία να περιορίζει επίσης τη χρήση εγκαταστάσεων εκτός ΕΟΧ από κρίσιμους τρίτους παρόχους υπηρεσιών ΤΠΕ. Η εν λόγω εξουσία θα μπορούσε να ασκηθεί σε συγκεκριμένες περιπτώσεις στις οποίες δεν υφίστανται διοικητικές συμφωνίες με τις οικείες αρχές τρίτων χωρών, κατά τα προβλεπόμενα στον προτεινόμενο κανονισμό ([96]), ή οι εκπρόσωποι των κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ δεν παρέχουν επαρκείς διαβεβαιώσεις βάσει του πλαισίου της οικείας τρίτης χώρας όσον αφορά την πρόσβαση στις πληροφορίες, στους χώρους, στην υποδομή και στο προσωπικό που απαιτούνται για την εκτέλεση των καθηκόντων επίβλεψης ή εποτείας.

4.4.4 Τέλος, το γεγονός ότι απαιτείται από τις αρμόδιες αρχές να δίνουν συνέχεια στις συστάσεις του κύριου εποπτικού φορέα ([97]) μπορεί να αποδειχθεί αναποτελεσματικό, καθώς οι αρμόδιες αρχές ενδέχεται να μην έχουν ολιστική άποψη για τους κινδύνους που δημιουργούνται από κάθε κρίσιμο τρίτο πάροχο υπηρεσιών ΤΠΕ. Επιπλέον, ενδέχεται να απαιτηθεί από τις αρμόδιες αρχές να λάβουν μέτρα κατά των εποπτευόμενων χρηματοπιστωτικών οντοτήτων τους όταν οι κρίσιμοι τρίτοι παρόχοι υπηρεσιών δεν επιδεικνύουν ενδιαφέρον για τις συστάσεις. Σύμφωνα με τον προτεινόμενο κανονισμό ([98]), οι αρμόδιες αρχές μπορούν να απαιτήσουν από τις εποπτευόμενες χρηματοπιστωτικές οντότητές τους να αναστείλουν προσωρινά τη χρήση ή την ανάπτυξη μιας υπηρεσίας που παρέχεται από τον κρίσιμο τρίτο ή να προβούν σε καταγγελία των υφιστάμενων συμβάσεων με κρίσιμους τρίτους παρόχους υπηρεσιών. Είναι δύσκολο να μεταφραστεί η προβλεπόμενη διαδικασία παρακολούθησης σε συγκεκριμένες ενέργειες. Συγκεκριμένα, δεν είναι σαφές εάν μια εποπτευόμενη χρηματοπιστωτική οντότητα θα είναι σε θέση να αναστείλει ή να καταγγείλει σύμβαση με κρίσιμο τρίτο πάροχο υπηρεσιών. Αυτό οφείλεται στο γεγονός ότι ο κρίσιμος τρίτος πάροχος υπηρεσιών ΤΠΕ θα μπορούσε να είναι σημαντικός πάροχος για τη συγκεκριμένη χρηματοπιστωτική οντότητα ή οφείλεται στις δαπάνες στις οποίες ενδέχεται να υποβληθεί η χρηματοπιστωτική οντότητα ή στη ζημία, συμβατική ή άλλης μορφής, που ενδέχεται να υποστεί αυτή λόγω της ανωτέρω αναστολής ή καταγγελίας. Επιπλέον, η εν λόγω προσέγγιση δεν υποστηρίζει τη σύγκλιση εποπτείας, καθώς οι αρμόδιες αρχές μπορούν να ερμηνεύσουν την ίδια σύσταση με διαφορετικό τρόπο. Αυτό θα μπορούσε τελικά να εμποδίσει την προβλεπόμενη εναρμόνιση και τη συνεπή προσέγγιση όσον αφορά την παρακολούθηση του κινδύνου κρίσιμων τρίτων παρόχων ΤΠΕ σε ενωσιακό επίπεδο. Λαμβανομένων υπόψη των προεκτεθέντων, τα νομοθετικά όργανα της Ένωσης μπορούν να εξετάσουν το ενδεχόμενο χορήγησης στους νόμιμους εποπτικούς φορείς ειδικών εκτελεστικών εξουσιών έναντι κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ, λαμβανομένων υπόψη των ορίων που επιβάλλονται από το δόγμα Meroni, όπως τα όρια αυτά εν μέρει μετριάστηκαν από το Δικαστήριο της Ευρωπαϊκής Ένωσης στην απόφασή του στην υπόθεση ESMA ([99]).

([93]) Βλέπε άρθρο 29 του προτεινόμενου κανονισμού.
([94]) Βλέπε άρθρο 29 παράγραφος 3 του προτεινόμενου κανονισμού.
([95]) Βλέπε άρθρο 35 του προτεινόμενου κανονισμού.
([96]) Βλέπε άρθρο 39 παράγραφος 1 του προτεινόμενου κανονισμού.
([97]) Βλέπε άρθρο 29 παράγραφος 4 και άρθρο 37 του προτεινόμενου κανονισμού.
([98]) Βλέπε άρθρο 37 παράγραφος 3 του προτεινόμενου κανονισμού.
([99]) Βλέπε απόφαση του Δικαστηρίου (τμήμα μείζονος συνθέσεως), της 22ας Ιανουαρίου 2014, Ηνωμένο Βασίλειο της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας κατά Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της Ευρωπαϊκής Ένωσης — κανονισμός (ΕΕ) αριθ. 236/2012 — Υπόθεση C-270/12.

Στις περιπτώσεις που η ΕΚΤ συνιστά την τροποποίηση του προτεινόμενου κανονισμού, συγκεκριμένες προτάσεις διατύπωσης περιλαμβάνονται σε τεχνικό κείμενο εργασίας και συνοδεύονται από τη σχετική αιτιολογία. Το τεχνικό κείμενο εργασίας διατίθεται στην αγγλική γλώσσα στο EUR-Lex.

Φρανκφούρτη, 4 Ιουνίου 2021.

Η Πρόεδρος της ΕΚΤ
Christine LAGARDE