

ΕΡΩΤΗΣΕΙΣ – ΑΠΑΝΤΗΣΕΙΣ

Για το νομοσχέδιο «Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών»

1. Ποιος είναι ο σκοπός του νομοσχεδίου;

Σκοπός του νομοσχεδίου είναι ο εκσυγχρονισμός της διαδικασίας άρσης του απορρήτου των επικοινωνιών με διασφάλιση όλων των απαιτούμενων εγγυήσεων, η αναδιάρθρωση της ΕΥΠ για τη βελτιστοποίηση της δράσης της, η ποινική μεταχείριση της εμπορίας, κατοχής και χρήσης λογισμικών παρακολούθησης, η οργανική και λειτουργική αναβάθμιση του επιπέδου κυβερνοασφάλειας στη χώρα και η βέλτιστη ενσωμάτωση στο εθνικό δίκαιο της Οδηγίας για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

2. Για ποιους λόγους μπορεί να γίνει νόμιμη άρση απορρήτου επικοινωνιών;

Σύμφωνα με το άρθρο 19 του Συντάγματος, το απόρρητο αίρεται για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων με απόφαση δικαστικής αρχής.

3. Τι σημαίνει «εθνική ασφάλεια» στη βάση της οποίας μπορεί να γίνει νόμιμη άρση απορρήτου;

Έως σήμερα δεν υφίσταται στον νόμο ορισμός. Με το νομοσχέδιο «λόγοι εθνικής ασφάλειας» χαρακτηρίζονται οι λόγοι που συνάπτονται με την προστασία των βασικών λειτουργιών του κράτους και των θεμελιωδών συμφερόντων του κοινωνικού συνόλου και περιλαμβάνουν την πρόληψη και την καταστολή δραστηριοτήτων ικανών να επιφέρουν πλήγμα στις συνταγματικές, πολιτικές, οικονομικές ή κοινωνικές δομές της χώρας όπως, ιδίως, λόγοι σχετικοί με την εθνική άμυνα και ασφάλεια, την εξωτερική πολιτική, την ενεργειακή ασφάλεια, την κυβερνοασφάλεια και την προστασία από άλλες υβριδικές απειλές, την προστασία του νομίματος και της εθνικής οικονομίας, την προστασία από ανθρωπιστική κρίση, τη δημόσια υγεία και την προστασία του περιβάλλοντος.

4. Ποια αρχή μπορεί να αιτηθεί άρση απορρήτου για λόγους εθνικής ασφάλειας;

Έως σήμερα την αίτηση θα μπορούσε να υποβάλλει κάθε δημόσια αρχή. Με το νομοσχέδιο τέτοια αίτηση μπορεί να ζητήσει μόνο η ΕΥΠ και η Αντιτρομοκρατική Υπηρεσία (Διεύθυνση Αντιμετώπισης Ειδικών Εγκλημάτων Βίας της Ελληνικής Αστυνομίας, «ΔΑΕΕΒ»).

5. Ποια είναι η διαδικασία για την άρση απορρήτου για λόγους εθνικής ασφάλειας;

Αίτηση της ΕΥΠ ή της Αντιτρομοκρατικής, κρίση εσωτερικού εισαγγελέα στην οικεία υπηρεσία και απόφαση αντεισαγγελέα του Αρείου Πάγου. Το δεύτερο εισαγγελικό φίλτρο προστέθηκε με την ΠΝΠ της 9/8/2022 που ουσιαστικά επανέφερε διάταξη που είχε καταργήσει ο ΣΥΡΙΖΑ το 2018.

6. Πως γίνεται η άρση απορρήτου για λόγους εθνικής ασφάλειας σε πολιτικά πρόσωπα;

Έως σήμερα δεν υφίσταται ειδική διαδικασία για πολιτικά πρόσωπα και ακολουθείται η συνήθης διαδικασία. Αποδείχθηκε ότι θα πρέπει να υπάρχουν ειδικές ασφαλιστικές δικλίδες. Τίθεται με το νομοσχέδιο ένα τριπλό φίλτρο εγγυήσεων: α) τη διαδικασία επισπεύδει μόνο η ΕΥΠ, β) θα πρέπει να δώσει άδεια ο Πρόεδρος της Βουλής πριν την διπλή εισαγγελική κρίση και γ) το αίτημα για την άρση οφείλει να στηρίζεται σε συγκεκριμένα στοιχεία που καθιστούν άμεση και εξαιρετικά πιθανή τη διακινδύνευση της εθνικής ασφάλειας.

7. Ποιοι λογίζονται για την εφαρμογή του νόμου πολιτικά πρόσωπα;

«Πολιτικά πρόσωπα» λογίζονται ο/η Πρόεδρος της Δημοκρατίας, τα μέλη της κυβέρνησης και οι υφυπουργοί, οι βουλευτές του εθνικού και του ευρωπαϊκού κοινοβουλίου, οι αρχηγοί των πολιτικών κομμάτων που εκπροσωπούνται στο εθνικό και το ευρωπαϊκό κοινοβούλιο και τα ανώτατα μονοπρόσωπα όργανα των ΟΤΑ Α' και Β' βαθμού.

8. Μπορεί το πρόσωπο το οποίο υπέστη την άρση απορρήτου για λόγους εθνικής ασφάλειας να ενημερώνεται εκ των υστέρων;

Έως το 2021, ήταν δυνατόν να ενημερώνεται κατά τη διακριτική ευχέρεια του αποφασίζοντος οργάνου, μόνο εφόσον δεν υφίστατο διακύβευση του σκοπού για τον οποίο διατάχθηκε η άρση. Έκτοτε δεν ήταν δυνατή η ενημέρωση όταν επρόκειτο για λόγους εθνικής ασφάλειας (ήταν όμως δυνατή για άρσεις προς διακρίβωση εγκλημάτων). Το ζήτημα αυτό είναι εξαιρετικά σύνθετο διότι πρέπει να συναιρεί δικαιώματα αλλά και την αποτελεσματικότητα της υπηρεσίας όταν πρόκειται για υψηλού επιπέδου κινδύνους. Με το νομοσχέδιο προτείνεται η ενημέρωση του υποκειμένου υπό την προϋπόθεση ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε η άρση και μετά την πάροδο 3 ετών από την παύση της. Η τριετία λογίζεται εύλογος χρόνος και ακολουθεί πρακτικές του εξωτερικού, ώστε να υφίσταται απόσταση από γεγονότα υψίστης εθνικής ασφαλείας (όπως εν προκειμένω τα γεγονότα του Έβρου και η κατασκοπεία της Ρόδου το 2020). Την ενημέρωση αποφασίζει τριμελές όργανο που απαρτίζεται από τον αρμόδιο εισαγγελέα, τον διοικητή της ΕΥΠ ή τον διευθυντή της ΔΑΕΕΒ και τον πρόεδρο της ΑΔΑΕ.

9. Διατηρεί αρχείο η αρχή που αιτήθηκε την άρση για λόγο εθνικής ασφάλειας;

Έως σήμερα, προβλέπεται η καταστροφή των αρχείων χωρίς όμως συγκεκριμένα χρονικά πλαίσια και συγκεκριμένες διαδικασίες. Πλέον η σχετική διαδικασία τυποποιείται. Για μεν το περιεχόμενο της παρακολούθησης, προβλέπεται καταρχήν αυτόματη διαγραφή μετά την πάροδο 6 μηνών από την παύση της άρσης. Για δε τον φάκελο με το υλικό τεκμηρίωσης για την άρση, προβλέπεται η καταστροφή του καταρχήν μετά την πάροδο 10 ετών από τη λήξη της άρσης. Προβλέπεται επιπλέον δυνατότητα πλήρους ψηφιοποίησης του αρχείου για εύκολη αναζήτηση και μείζονα ασφάλεια.

10. Για τη διακρίβωση ποινών εγκλημάτων μπορεί να γίνει άρση απορρήτου;

Έως σήμερα ο κατάλογος ήταν εξαιρετικά ευρύς και περιλάμβανε κακουργήματα και πλημμελήματα του ποινικού κώδικα και ειδικών ποινικών νόμων. Ο κατάλογος αυτός εξορθολογίζεται ώστε να περιλάβει καταρχήν όλα τα κακουργήματα και από τα πλημμελήματα μόνο όσα

φέρουν ιδιαίτερη απαξία (πχ κατά ανηλίκων, εμπρησμοί, εγκληματική συμμορία) αφαιρώντας τους περισσότερους ειδικούς νόμους. Για παράδειγμα, δεν μπορεί να διαταχθεί η άρση για απλή κλοπή ή απάτη.

11. Με ποια διαδικασία διατάσσεται η άρση για τη διακρίβωση εγκλημάτων;

Η σχετική διαδικασία δεν αλλάζει. Η άρση επιβάλλεται με βούλευμα του Συμβουλίου Εφετών ή Πλημμελειοδικών μετά από αίτηση του εισαγγελέα ή του ανακριτή. Μόνο σε εξαιρετικά επείγουσες περιπτώσεις, την άρση μπορεί να διατάξει ο εισαγγελέας και ο ανακριτής που στη συνέχεια υποχρεούνται να εισαγάγουν το ζήτημα με σχετική αίτηση στο Συμβούλιο μέσα σε προθεσμία 3 ημερών.

12. Μπορεί το πρόσωπο το οποίο υπέστη την άρση απορρήτου για λόγους διακρίβωσης εγκλημάτων να ενημερώνεται εκ των υστέρων;

Δεν αλλάζει κάτι. Η ΑΔΑΕ αποφασίζει μετά τη λήξη του μέτρου την ενημέρωση του υποκειμένου, με τη σύμφωνη γνώμη του Εισαγγελέα του Αρείου Πάγου και υπό την προϋπόθεση, ότι δεν διακυβεύεται ο σκοπός για τον οποίο διατάχθηκε. Το μόνο που προστίθεται είναι ότι η ΑΔΑΕ απαντά επί του αιτήματος εντός 3 μηνών, άλλως η αίτηση θεωρείται ότι έχει απορριφθεί.

13. Υπάρχει ανώτατο χρονικό όριο άρσης απορρήτου;

Έως σήμερα οι άρσεις διατάσσονται για δίμηνο με δυνατότητα ανανέωσης, δεν υπάρχει απώτατο χρονικό όριο για άρσεις λόγω εθνικής ασφάλειας και υπάρχει όριο 10 μηνών για τη διακρίβωση εγκλημάτων. Πλέον το όριο των 10 μηνών καταλαμβάνει και τις άρσεις λόγω εθνικής ασφάλειας, εκτός εάν η αίτηση στηρίζεται σε συγκεκριμένα στοιχεία που καθιστούν άμεση και εξαιρετικά πιθανή τη διακινδύνευση της εθνικής ασφάλειας .

14. Γιατί θα πρέπει να υπάρχει ειδικός εισαγγελέας στην ΕΥΠ και στην Αντιτρομοκρατική;

Η ύπαρξη ειδικών εισαγγελέων ενισχύει την εξειδίκευση των προσώπων αλλά και τη στεγανοποίηση των πληροφοριών. Σε κάθε περίπτωση απαιτείται για την άρση απορρήτου λόγω εθνικής ασφάλειας και

δεύτερος εισαγγελέας ώστε να μη λειτουργεί το σύστημα ιδρυματικά. Για τον ίδιο λόγο, οι θητείες των επιτόπιων εισαγγελέων είναι τριετείς μη ανανεούμενες (ενώ ως σήμερα η θητεία του εισαγγελέα της αντιτρομοκρατικής μπορεί να ανανεωθεί).

15. Τι προβλέπεται για τις απαγορεύσεις στην κατοχή, εμπορία, διάθεση και χρήση απαγορευμένων λογισμικών;

Έως το 2019 η παράνομη υποκλοπή ήταν κακούργημα και τιμωρείτο με κάθειρξη έως 10 έτη, ενώ η κατοχή και εμπορία παράνομων λογισμικών ήταν πλημμέλημα και τιμωρείτο με φυλάκιση έως 2 έτη. Λίγες μέρες πριν τη διάλυση της Βουλής για τις εκλογές του 2019 και ενόσω ο ΣΥΡΙΖΑ γνώριζε την ύπαρξη στην Ελλάδα παράνομων λογισμικών, άλλαξε ακατανόητα ο Ποινικός Κώδικας με αποτέλεσμα η μεν υποκλοπή πλέον να τιμωρείται με φυλάκιση από 10 μέρες έως 5 έτη, η δε κατοχή και εμπορία αποποινικοποιήθηκε. Με τις προτεινόμενες διατάξεις επανέρχεται ως είχε το κακούργημα για τη χρήση παράνομων λογισμικών και συσκευών και το πλημμέλημα της εμπορίας και κατοχής με ποινή 1-5 έτη.

16. Πώς θα γνωρίζει κάποιος τι συνιστά απαγορευμένο λογισμικό και συσκευή;

Απαγορευμένα λογισμικά ή συσκευές παρακολούθησης λογίζονται λογισμικά ή συσκευές με δυνατότητα υποκλοπής, καταγραφής και κάθε είδους άντλησης περιεχομένου ή και δεδομένων επικοινωνίας (κίνησης και θέσης), τα οποία καθορίζονται με απόφαση του Διοικητή της ΕΥΠ που θα δημοσιευτεί μέσα σε 3 ημέρες από την ισχύ του νόμου. Ο κατάλογος απαγορευμένων λογισμικών ή συσκευών παρακολούθησης επικαιροποιείται με απόφαση του Διοικητή της ΕΥΠ το αργότερο κάθε 6 μήνες. Επιπλέον, με ανακοίνωση του Διοικητή της ΕΥΠ, που αναρτάται στον ιστοχώρο της Υπηρεσίας ενημερώνεται το κοινό για τα απαγορευμένα λογισμικά, τον τρόπο δράσης τους και τα μέτρα προστασίας που δύναται να λάβει έναντι αυτών.

17. Απαγορεύσεις για κατοχή και εμπορία κακόβουλων λογισμικών δεν υπάρχουν ήδη;

Όχι για παραβίαση απορρήτου ιδιωτικών επικοινωνιών. Το ισχύον άρθρο 292Α δεν καλύπτει απολύτως τη διάταξη που φέρνουμε. Ανήκει στο

κεφάλαιο «Εγκλήματα κατά τηλεπικοινωνιών» του Ποινικού Κώδικα και αναφέρεται σε πρόσβαση σε σύνδεση ή σε δίκτυο με τρόπο που θέτει σε συστημικό κίνδυνο τη φυσική ασφάλεια του δικτύου τηλεφωνικών επικοινωνιών (αρμοδιότητας ΕΕΤΤ). Αντιθέτως, η διάταξη του νέου νομοσχεδίου για τα κακόβουλα λογισμικά ανήκει στο κεφάλαιο «Προσβολές ατομικού απορρήτου και επικοινωνίας» και αφορά κάθε λογισμικό ή συσκευή που παρεμβαίνει σε ιδιωτικές επικοινωνίες (αρμοδιότητας ΑΔΑΕ). Συνεπώς, οι δύο διατάξεις έχουν διαφορετικό σκοπό. Για τον λόγο αυτό εξάλλου συνυπάρχουν και σήμερα, από μακρού χρόνου, στον ισχύοντα ποινικό κώδικα οι δύο διαφορετικές διατάξεις. Αυτό το οποίο προτείνουμε με το νομοσχέδιο είναι να επανέλθει με αυστηρότερο και αναβαθμισμένο ποινικά περιεχόμενο η διάταξη που κατήργησε ο ΣΥΡΙΖΑ και αφορά την καθολική απαγόρευση εμπορίας, διάθεσης και κατοχής λογισμικών παρακολούθησης ατομικών επικοινωνιών.

18. Το δημόσιο θα μπορεί να προμηθεύεται κατασκοπευτικά λογισμικά;

Το δημόσιο θα μπορεί να προμηθεύεται κατασκοπευτικά λογισμικά υπό προϋποθέσεις που θα καθορίζονται με προεδρικό διάταγμα των συναρμόδιων υπουργών, που θα έχει τύχει της προβλεπόμενης επεξεργασίας του Συμβουλίου της Επικρατείας.

19. Γιατί λέμε ότι για πρώτη φορά εισάγεται στην Ελλάδα καθολική απαγόρευση της κατοχής και εμπορίας κακόβουλων λογισμικών, εφόσον υπήρχαν και στο παρελθόν κάποιες διατάξεις;

Η διάταξη που κατήργησε ο ΣΥΡΙΖΑ πράγματι αφορούσε κατοχή και εμπορία κακόβουλων λογισμικών, όμως ήταν περιορισμένης εμβέλειας και ανεφάρμοστη στην πράξη. Πρώτον, αναφερόταν σε κατοχή και χρήση «χωρίς δικαίωμα», χωρίς να προσδιορίζεται ποιος είχε δικαίωμα. Δεύτερον, απαιτούσε η κατοχή και εμπορία να γίνεται για «σκοπό» διάπραξης του εγκλήματος της υποκλοπής, που όμως στην πράξη ήταν αδύνατον να αποδειχθεί. Τρίτον, η διάταξη δε προσδιόριζε ποια πράγματι ήταν τα απαγορευμένα λογισμικά και συσκευές. Με τη νέα διάταξη όποιος κατέχει ή εμπορεύεται τα αναγραφόμενα στον κατάλογο λογισμικά και συσκευές τιμωρείται με βαριές ποινές χωρίς να απαιτείται η συνδρομή οποιασδήποτε άλλης προϋπόθεσης, άρα καθολικά.

20. Τι αλλάζει στη διοίκηση της ΕΥΠ;

Έως σήμερα ο διοικητής και οι υποδιοικητές μπορεί να προέρχονται από τον δημόσιο ή τον ιδιωτικό τομέα. Με το προτεινόμενο νομοσχέδιο, Διοικητής ορίζεται πρόσωπο προερχόμενο από το διπλωματικό σώμα ή απόστρατος ανώτατος αξιωματικός. Υποδιοικητές μπορεί να είναι κάποιιοι από τους ανωτέρω, καθώς και υπάλληλοι και λειτουργοί του δημοσίου και του ευρύτερου δημοσίου τομέα. Επιπλέον, ο αριθμός των υποδιοικητών περιορίζεται από 3 που είναι σήμερα σε 2.

21. Τι αλλάζει στην οργάνωση της ΕΥΠ;

Προστίθενται 3 νέα δομές. α) Η Ακαδημία Πληροφοριών και Αντικατασκοπείας με αποστολή την εκπαίδευση, επιμόρφωση και εξειδίκευση του προσωπικού της ΕΥΠ για την αποτελεσματικότερη εκτέλεση των καθηκόντων του. β) Η Μονάδα Εσωτερικού Ελέγχου, η οποία είναι αρμόδια μεταξύ άλλων για τον εσωτερικό έλεγχο της ΕΥΠ. γ) Το Γραφείο Τύπου και Επικοινωνίας, με αρμοδιότητα για την προβολή του έργου της υπηρεσίας και για την ενημέρωση της κοινωνίας για τις δράσεις της και για τυχόν κινδύνους για την εθνική ασφάλεια.

22. Τι αλλάζει στη λειτουργία της ΕΥΠ;

Πρώτον, η Αρχή Ασφαλείας Πληροφοριών (INFOSEC) της ΕΥΠ καθίσταται αρμόδια για τη σύνταξη πολιτικών ασφαλείας και οδηγιών διαχείρισης των διαβαθμισμένων πληροφοριών σε όλα τα δίκτυα και τους χώρους της Προεδρίας της Κυβέρνησης και των Υπουργείων σε συνεργασία μαζί τους, καθώς και για τη συνεχή ενημέρωσή τους σε θέματα ασφαλείας. Δεύτερον, καταργείται η δυνατότητα απόρρητων συμβάσεων στο Κέντρο Τεχνολογικής Υποστήριξης, Ανάπτυξης και Καινοτομίας (ΚΕ.Τ.Υ.Α.Κ.)

23. Πως βελτιώνεται το επίπεδο κυβερνοασφάλειας στη χώρα;

Το πιο σημαντικό πρόβλημα είναι η πολυδιάσπαση των δομών κυβερνοασφάλειας στη χώρα. Για τον λόγο αυτό συστήνεται Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας, που λειτουργεί ως συντονιστικό όργανο μεταξύ: α) της Γενικής Διεύθυνσης Κυβερνοασφάλειας της Γενικής Γραμματείας Τηλεπικοινωνιών και Ταχυδρομείων του Υπουργείου Ψηφιακής Διακυβέρνησης, που έχει ορισθεί ως Εθνική Αρχή της Κυβερνοασφάλειας, β) της Διεύθυνσης

Κυβερνοάμυνας του ΓΕΕΘΑ, που έχει ορισθεί ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών, γ) της Διεύθυνσης Κυβερνοχώρου της ΕΥΠ ως ομάδα αντιμετώπισης ηλεκτρονικών επιθέσεων (Εθνικό CERT) και δ) της Ελληνικής Αστυνομίας. Οι αρμοδιότητες της Επιτροπής είναι: α) να παρέχει κατευθύνσεις σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο, β) να συντονίζει, παρακολουθεί και αξιολογεί την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας, γ) να εγκρίνει το Εθνικό Σχέδιο Έκτακτης Ανάγκης, δ) να εισηγείται στο ΚΥ.Σ.Ε.Α. οποιοδήποτε θέμα άπτεται της Κυβερνοασφάλειας και ε) να αίρει τυχόν διαφωνίες ως προς τις αρμοδιότητες και τους ρόλους των φορέων Κυβερνοασφάλειας.

24. Υπάρχει σύστημα μελέτης και έγκαιρης προειδοποίησης κινδύνου για την κυβερνοασφάλεια;

Σύμφωνα με το νομοσχέδιο, η Εθνική Αρχή της Κυβερνοασφάλειας σε συνεργασία με τη Διεύθυνση Κυβερνοχώρου της ΕΥΠ, τη Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ, την Ελληνική Αστυνομία και κάθε άλλο αρμόδιο φορέα, καταρτίζει Εθνικό Σχέδιο Αποτίμησης Επικινδυνότητας Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών, το οποίο διαβαθμίζεται σύμφωνα με τον Εθνικό Κανονισμό Ασφαλείας. Το Σχέδιο περιλαμβάνει την αναγνώριση, ανάλυση και αποτίμηση των κινδύνων και των επιπτώσεων τους για την ασφάλεια των συστημάτων τεχνολογίας πληροφορικής και επικοινωνιών σε εθνικό επίπεδο. Για την κατάρτιση του Σχεδίου λαμβάνεται υπόψη κάθε κατηγορία πιθανής απειλής, και ιδίως απειλές που σχετίζονται με κακόβουλες ενέργειες, φυσικά φαινόμενα, τεχνικές αστοχίες, δυσλειτουργίες ή ανθρώπινα λάθη, με σκοπό την αξιολόγηση της έκτασης και της κρισιμότητας των επιπτώσεων των απειλών αυτών σε εθνικό επίπεδο. Επιπλέον, η Εθνική Αρχή της Κυβερνοασφάλειας και η Διεύθυνση Κυβερνοχώρου μεριμνούν για την παρακολούθηση γνωστών απειλών και ευπαθειών συστημάτων πληροφορικής και επικοινωνιών και την παροχή ενημέρωσης σχετικά με αυτές.

25. Πως διασφαλίζεται περαιτέρω η προστασία των δεδομένων προσωπικού χαρακτήρα;

Με τον ν. 4624/2019 (μόλις ο τέταρτος νόμος που ψηφίστηκε από τη νέα Βουλή που προέκυψε από τις εκλογές του 2019), ενσωματώθηκε στην ελληνική έννομη τάξη ο Κανονισμός 2016/679 και η Οδηγία 2016/680. Το

πακέτο αυτό ήταν υπερήμερο από μακρού χρόνου λόγω της αδράνειας του ΣΥΡΙΖΑ απέναντι σε αυτή την ενωσιακή υποχρέωση. Κατά τη διάρκεια του χρόνου που πέρασε από τη δημοσίευση του νόμου στις 29.08.2019 διαπιστώθηκαν στην πράξη αλλά και από την Ευρωπαϊκή Επιτροπή ορισμένα ζητήματα για τη βελτίωση του υφιστάμενου πλαισίου στην Ελλάδα. Με το προτεινόμενο νομοσχέδιο και συγκεκριμένα 12 παρεμβάσεις καλύπτονται κενά και αίρονται σχετικές ασάφειες προς την κατεύθυνση της ενίσχυση του βασικού δικαιώματος προστασίας προσωπικών δεδομένων. Επιπλέον, για την παρακολούθηση των σχετικών πολιτικών, συστήνεται στο Υπουργείο Δικαιοσύνης Μόνιμη Επιστημονική Επιτροπή Προσωπικών Δεδομένων με αποστολή: α) την παρακολούθηση των επιστημονικών και νομολογιακών εξελίξεων και του εθνικού και ενωσιακού νομικού πλαισίου προστασίας των δεδομένων προσωπικού χαρακτήρα, β) την υποβολή τεκμηριωμένων προτάσεων για την ανάληψη νομοθετικής δράσης στον τομέα αυτό, γ) την άσκηση καθηκόντων νομοπαρασκευαστικού έργου και δ) την αντιπροσώπευση του Υπουργείου Δικαιοσύνης σε διεθνή όργανα. Τέλος προβλέπεται ότι με διάταξη Εισαγγελέα, η Ελληνική Αστυνομία προβαίνει σε ανακοίνωση ή δημοσιοποίηση των στοιχείων της ταυτότητας, της εικόνας και της ποινικής δίωξης κατηγορουμένου ή καταδικασθέντος για κακούργημα, για πλημμέλημα κατά της γενετήσιας ελευθερίας, καθώς και για πλημμέλημα το οποίο τιμωρείται με ποινή φυλάκισης τουλάχιστον δυο 2 ετών.