ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΤΟΥΡΙΣΜΟΥ

ΠΠΣ. ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΨΗΦΙΑΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ – Ο ΡΟΛΟΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR)»

ΧΡΗΣΤΟΣ ΛΟΥΛΟΥΔΑΣ ΑΜ 17059

ΒΙΡΓΙΝΙΑ – ΤΡΙΣΕΥΓΕΝΗ ΨΑΡΟΠΟΥΛΟΥ ΑΜ 17159

ΑΔΑΜΑΝΤΙΑ ΜΙΧΑΛΟΠΟΥΛΟΥ ΑΜ 17075

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ

ΒΑΘΗ – ΣΑΡΑΒΑ ΠΑΝΑΓΙΩΤΑ

ΠΑΤΡΑ 2021

UNIVERSITY OF PATRAS

SCHOOL OF ECONOMICS AND BUSINESS

DEPARTMENT OF TOURISM MANAGEMENT

FORMER DEPARTMENT OF ACCOUNTING AND FINANCE

THESIS:

«ECONOMICAL AND DIGITAL CRIME- THE ROLE OF GENERAL DATA PROTECTION (GDPR) »

CHRISTOS LOULOUDAS

VIRGINIA PSAROPOULOU

ADAMANTIA MICHALOPOULOU

PATRAS 2021

ΠΡΟΛΟΓΟΣ

Τα προβλήματα που δημιουργούν οι αλλεπάλληλες παραβάσεις τόσο στον οικονομικό όσο και στον ψηφιακό κόσμο καθώς και οι τρόποι με τους οποίους συνήθως γίνονται αλλά και οι τρόποι αντιμετώπισης αυτών των φαινομένων στις σύγχρονες κοινωνίες θα αναλυθούν με τον καλύτερα δυνατό τρόπο στην παρούσα εργασία. Επιπλέον με την βοήθεια του Ευρωπαϊκού κανονισμού προστασίας προσωπικών δεδομένων (GDPR) θα εξηγήσουμε πως επιδρά σε όλες αυτές τις παραβατικές συμπεριφορές αλλά και την χρησιμότητα και τη διασφάλιση ενάντια σε όλες αυτές τις προκλήσεις μέσα από 3 κεφάλαια και με το τελευταίο κεφάλαιο να αναφέρεται στην βιβλιογραφική αναφορά που χρησιμοποιήθηκε.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία πραγματεύεται το ζήτημα της «οικονομικής και ψηφιακής παραβατικότητας δίνοντας έμφαση στο ρόλο της προστασίας προσωπικών δεδομένων GDPR». Αρχικά, θα πραγματοποιηθεί ανάλυση της έννοιας της οικονομικής παραβατικότητας αλλά και των μορφών της που συναντώνται στις σύγχρονες κοινωνίες. Επιπρόσθετα, θα γίνει αναφορά και σε ορισμένους ενδεικτικούς τρόπους αντιμετώπισης της.

Κατόπιν, θα αναλυθεί κατά τον ίδιο τρόπο και η ψηφιακή παραβατικότητα, δηλαδή η έννοια, τα χαρακτηριστικά, οι κατηγορίες αλλά και οι τρόποι αντιμετώπισης της. Επιπλέον, θα αναγραφούν και κάποια ενδεικτικά πρόσφατα στοιχεία στον Ελλαδικό χώρο από την ελληνική αστυνομία.

Έπειτα, θα αναλυθεί ο γενικός κανονισμός προστασίας προσωπικών δεδομένων GDPR όπου σε γενικές γραμμές θα αναλυθούν τα κύρια σημεία του κανονισμού, ο τρόπος που εφαρμόζεται, τι εξαιρείται αλλά και ποιες είναι οι κυρώσεις που επιβάλλονται σε περίπτωση παραβίασης των σχετικών άρθρων.

Τέλος, μετά από την παραπάνω ανάλυση θα ακολουθήσει το κομμάτι του ρόλου που διαδραματίζει ο κανονισμός τόσο στην ψηφιακή όσο και την οικονομική παραβατικότητα αλλά και τα αρνητικά και τα θετικά στοιχεία που βοηθά ο κανονισμός.

Λέξεις -Κλειδιά: Οικονομική παραβατικότητα, Ψηφιακή παραβατικότητα, GDPR, Διαδίκτυο, καταναλωτής

ABSTRACT

This dissertation addresses the issue of economic and digital violation with emphasis put on the role of GDPR personal data protection. Initially, an analysis will be made of the concept of economic delinquency and its forms found in modern societies. In addition, reference will be made to some indicative ways of dealing with it. Then, digital delinquency will be analyzed in the same way, for example the concept, the characteristics, the categories but also the ways of dealing with it. In addition, some indicative recent data will be listed in Greece by the Greek police. Then, the general regulation of personal data protection GDPR will be analyzed where in general will be analyzed the main points of the regulation, the way it is applied, what is exempted and what are the sanctions imposed in case of violation of the relevant articles. Finally, after the above analysis will follow the part of the role that the regulation plays in both digital and financial delinquency, as well as the negative and positive elements that the regulation helps.

Key Words: Economic delinquency, Digital delinquency, GDPR, Internet, consumer

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Θεμελιώδες δικαίωμα για τους πολίτες αποτελεί το δικαίωμα προστασίας της προσωπικής ζωής. Εδώ και πολλά χρόνιά η Ευρωπαϊκή ένωση προσπαθούσε με διατάξεις και νόμους να επιτύχει την προστασία των δεδομένων των πολίτων της. Με επίπονες και πολύχρονες διαδικασίες τελικά ορίστηκε το 2016 ο γενικός κανονισμός προστασίας προσωπικών δεδομένων GDPR. Η αναγκαστική εκτέλεση της ορίστηκε στα κράτη- μέλη το 2018 .

Ο πρωταρχικός σκοπός του GDPR είναι η προστασία των Ευρωπαίων πολιτών από την μη εξουσιοδοτημένη χρήση των ευαίσθητων προσωπικών δεδομένων τους από μη έμπιστα άτομα . Γιατί όπως άλλωστε ορίζει και ο κανονισμός ορίστηκε για *«την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών»* (Ευρωπαϊκό κοινοβούλιο 31995L0046 - Οδηγία 95/46 ΕΚ 1995)

Παρόλα αυτά και σε άλλους τομείς βοήθησε ο κανονισμός προστασίας προσωπικών δεδομένων. Πιο συγκεκριμένα για την πάταξη πολλών ηλεκτρονικών εγκλημάτων που με την ευρεία διάδοση του διαδικτύου αυξήθηκε την τελευταία δεκαετία κατά υψηλό ποσοστό. Επιπλέον, δίδεται στους Ευρωπαίους πολίτες η δυνατότητα να νιώθουν ασφαλείς με τις προσωπικές τους πληροφορίες που κοινοποιούν σε διάφορες ιστοσελίδες καθώς υπάρχει στον κανονισμό ειδικό κανονιστικό καθεστώς ελέγχου για την ορθή και πιστή υπακοή στον κανονισμό από όλες της επιχειρήσεις που δραστηριοποιούνται μέσω διαδικτύου στην Ευρώπη και διαδικασία επιβολής κυρώσεων σε περίπτωση παραβίασης. Επιπροσθέτως, ο κανονισμός σε γενικές γραμμές βοήθησε και τις επιχειρήσεις στον τομέα διαχείρισης όλων αυτών των προσωπικών πληροφοριών που διαθέτουν. Δηλαδή στο να αναθεωρήσουν ορισμένες στρατηγικές τους ως προς την διαχείριση αυτού του μεγάλου όγκου πληροφοριών και να εστιάσουν σε νέες τεχνικές απόκρυψης των ευαίσθητων στοιχείων.

Στην παρούσα πτυχιακή εργασία προσπαθήσαμε κατά το μέτρο του δυνατού να αποτυπώσουμε όλα τα παραπάνω με σχετικά μικρή βιβλιογραφική αναφορά καθώς το παρών θέμα παίρνει πολλές διαστάσεις για τις οποίες αρκετές φορές οι απόψεις διίστανται.

Η δομή της εργασίας μας έχει ως εξής:

Στο 1^{ο} κεφάλαιο αναφερόμαστε στην οικονομική παραβατικότητα των επιχειρήσεων ,μια ευρέως δυναμική κατάσταση που επικρατεί στις σύγχρονες κοινωνίες για πολλούς και διαφόρους λόγους αλλά κυρίως για την μεγιστοποίηση του κέρδους. Πιο συγκεκριμένα αναγράφουμε τον ορισμό από διάφορες οπτικές πλευρές , τις μορφές που επικρατούν στις

σύγχρονες κοινωνίες και έπειτα ορισμένους κατά την γνώμη ορισμένων επιστημόνων τρόπους αντιμετώπισης αυτού του φαινομένου.

Στο 2ο κεφάλαιο εστιάζουμε σε ένα ακόμη μεγάλο πρόβλημα των σύγχρονων κοινωνιών ,την ψηφιακή παραβατικότητα. Εστιάζουμε στον ορισμό της καθώς και στα χαρακτηριστικά με τα οποία εμφανίζεται , κατηγοριοποιούμε τις διάφορες μορφές με την οποία εμφανίζεται και επίσης και εδώ παραθέτουμε μερικούς τρόπους αντιμετώπισης της . Τελικά ως κάτι αξιοσημείωτο αναγράφουμε μερικά πρόσφατα στατιστικά στοιχεία καθώς και μια από τις περιζήτητες και παγκόσμια σύγχρονη απάτη τα κρυπτονομίσματα.

Στο 3ο κεφάλαιο παρουσιάζουμε τον γενικό κανονισμό προστασίας προσωπικών δεδομένων GDPR όπου μέσα από 5 ΥΠΟ ενότητες παρουσιάζουμε συνοπτικά ότι ορίζει ο κανονισμός όπως ορίστηκε από την Ευρωπαϊκή κομισιόν . Επιπροσθέτως, εστιάζουμε στις βασικές έννοιες του κανονισμού , τους υπεύθυνους που καλύπτει ο κανονισμός , μερικές εξαιρέσεις που ορίζει ο κανονισμός, τα πεδία στα οποία εφαρμόζεται και στο τέλος αναφέρουμε την διαδικασία που ορίζεται σε περίπτωση που κάποιο πρόσωπο ή επιχείρηση παραβιάσει κάποιον κανόνα καθώς και τα χρηματικά πρόστιμα που προβλέπονται.

Τέλος , στο κεφάλαιο αυτό καταγράφουμε και λίγους από τους θετικούς αλλά και τους αρνητικούς ρόλους που διαδραματίζει το GDPR τόσο σε οικονομικό όσο και σε ψηφιακό επίπεδο.

ΚΕΦΑΛΑΙΟ 1 – ΟΙΚΟΝΟΜΙΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

1.1 ΕΝΝΟΙΑ ΤΗΣ ΟΙΚΟΝΟΜΙΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Αρχικά η επιστημονική προσέγγιση περί οικονομικών εγκλημάτων ξεκίνησε το 1939 στις Ηνωμένες πολιτείες από τον E Sutherland. ***«Παραβατικότητα ή αλλιώς εγκληματικότητα*** ή ακόμα και ***αποκλίνουσα συμπεριφορά*** όπως θεωρούν οι κοινωνιολόγοι θεωρούν ότι είναι μια συμπεριφορά που χαρακτηρίζεται από το κοινωνικό σύνολο ως αντικοινωνική και δεν αρμόζει στην επικρατούσα ηθική και φυσικά συνεπάγεται με την επιβολή κυρώσεων.» Για έναν νομικό το έγκλημα - παράβαση είναι η καταπάτηση ενός κανόνα του ποινικού δικαίου. Παρόλα αυτά αυτές οι δυο προαναφερθείσες έννοιες συναντώνται με τον όρο «αποκλίνουσα συμπεριφορά». Συμπερασματικά, ο ορισμός της παραβατικότητας δεν διαθέτει έναν συγκεκριμένο ορισμό γιατί υπάρχουν πολλές προσεγγίσεις από πολλούς κλάδους (νομικούς –κοινωνιολόγους) (Τσουραμάνης ,1996)

Μερικά από τα οικονομικά εγκλήματα είναι τα γνωστά κατά τον ποινικό κώδικα εγκλήματα ιδιοκτησίας κυρίως αναφερόμενα στο περιουσιακό δίκαιο. Ακόμη, στα πλαίσια της παραβατικότητας λογίζονται πράξεις που προβλέπονται από συγκεκριμένους νομούς χωρίς να αφορούν άμεσα οικονομικά ζητήματα αλλά αναφέρονται κυρίως σε οικονομική δραστηριότητα με ορισμένα πρόσωπα πχ η απαγόρευση διακίνησης όπλων σε τριτοκοσμικές χώρες. Επιπλέον, στα πλαίσια της παραβατικότητας ανήκουν και εγκλήματα που συμπεριλαμβάνονται στον ποινικό κώδικα που σχετίζονται με την οικονομία πχ φορολογική απατή, trade marks. (Κουράκης,1982)

Συμπληρωματικά υπάρχουν και ορισμένα σύγχρονα οικονομικά εγκλήματα όπου αναφέρθηκαν επίσης και στο Συμβούλιο της Ευρώπης την 25η Ιουνίου 1981 και αφορούν τα εγκλήματα περί των διακινήσεων παράνομων προϊόντων και υλικών, εταιρείες φαντάσματά όπως επίσης και ο αθέμιτος ανταγωνισμός μέσω κατάχρησης δικαιωμάτων από μεγάλες πολυεθνικές εταιρείες. Επιπρόσθετα, στα οικονομικά εγκλήματα συγκαταλέγεται και η μη τήρηση λογιστικών βιβλίων και η αλλοίωση αποτελεσμάτων ισολογισμών, οι παραβάσεις φορολογικού κώδικα και η αποφυγή πληρωμής των κοινωνικών δαπανών από επιχειρήσεις και τέλος οι παραβάσεις σε σχέση με τους εκτελωνισμούς (αποφυγή δασμών, παράβαση άλλων περιορισμών που ορίζονται από τα διαφορά κράτη). (Δημόπουλος , 1989)

Επεξηγηματικά υπάρχει και ο εξής ορισμός κατά τον Κουράκη (1982)

« Οικονομική εγκληματικότητα είναι καθ' αυτόν το σύνολο των αθέμιτων δραστηριοτήτων η οποία συμβαίνει μεταξύ των επιχειρήσεων η οποία σε συνέχεια βλάπτει την καλή λειτουργία της οικονομίας ή των σημαντικών λειτουργικών κλάδων.»(Κουράκης ,1982)

Συμπερασματικά, ο όρος οικονομική εγκληματικότητα δεν μπορεί να αποδοθεί με έναν σαφή ορισμό λόγω του πολυσυνθέτου αυτού θέματος αλλά και των διαφόρων προσεγγίσεων που υπάρχουν από διάφορες επιστήμες και επιστήμονες σε διάφορους χρονικούς ορίζοντες. Εν κατακλείδι, το θέμα υφίσταται περαιτέρω διερεύνησης λόγω των διαφόρων αλλαγών που υφίσταται η οικονομία αλλά και η κοινωνία σε βάθος χρόνου (Τσουραμάνης 1996).

1.2 ΜΟΡΦΕΣ ΟΙΚΟΝΟΜΙΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Σε αυτή την υπό-ενότητα θα αναφερθούν τρεις κυρίαρχες μορφές με βάση τα σύγχρονα δεδομένα των νέων κοινωνιών:

α) η οικονομική παραβατικότητα των επιχειρήσεων αλλά και την

β) η φοροδιαφυγή

γ) η εξαπάτηση των καταναλωτών

δ) η μόλυνση του περιβάλλοντος

1.2.1 ΟΙΚΟΝΟΜΙΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Ξεκινώντας με την οικονομική παραβατικότητα των επιχειρήσεων, αρχικά αξίζει να αναφερθεί ότι μετά τον β παγκόσμιο πόλεμο η τεχνολογική υπερανάπτυξη έχει οδηγήσει

ειδικά τις ανεπτυγμένες χώρες στην ανάπτυξη πολλών επιχειρήσεων με κοινό σκοπό την μεγιστοποίηση των κερδών τους αλλά και την ικανοποίηση των διαφόρων στόχων τους (Τσουραμάνης,1996).

Ωστόσο, επιχείρηση ονομάζεται μια παραγωγική- οικονομική μονάδα που συνδυάζει και αξιοποιεί τους παραγωγικούς συντελεστές προκειμένου να παράγει προϊόντα ή υπηρεσίες με σκοπό την διάθεση τους προς τον τελικό καταναλωτή.

Όμως αυτή η δραστηριοποίηση των διαφόρων επιχειρήσεων δεν έχει πάντα κοινωνικά αποδέκτες συμπεριφορές. Θα ήταν αμελητέο να αναφερθεί πως σχεδόν όλες οι επιχειρήσεις παραβαίνουν έναν η περισσότερους κανόνες της εκάστοτε νομοθεσίας προκειμένου να επιτύχουν τους στόχους τους αλλά και να επιδείξουν ότι υπερέχουν έναντι σε άλλες ανταγωνίστριες επιχειρήσεις. Εννοείται πως για να παραβαίνουν την εκάστοτε νομοθεσία διαθέτουν και τα κατάλληλα μέσα για να το επιτύχουν όπως για παράδειγμα δικηγόρους υψηλού κυρούς που γνωρίζουν άριστα την νομοθεσία και τους τρόπους που θα αξιοποιήσουν για την κάλυψη των διαφόρων παραβιάσεων χρησιμοποιώντας νομικούς κώδικες πως ονομάζονται ή η οικονομική εξάρτηση πολλών από τα ΜΜΕ από τέτοιες επιχειρήσεις με αποτέλεσμα την ευνοϊκή αποδοχή των πράξεων αυτών από το ευρύ κοινό μέσω της προπαγάνδας)

Μιλώντας για οικονομική παραβατικότητα των επιχειρήσεων όπως αναφέραμε και παραπάνω αυτή οφείλεται κυρίως για την μεγιστοποίηση του κέρδους και ικανοποίηση των διαφόρων στόχων που θέτει η κάθε επιχείρηση. Οι παραβιάσεις αυτές αφορούν κυρίως :

Α) Παραβίαση νόμων για βιομηχανική ιδιοκτησία

Τα δικαιώματα βιομηχανικής ιδιοκτησίας προστατεύουν τα άυλα περιουσιακά στοιχεία. Τα δικαιώματα βιομηχανικής ιδιοκτησίας και τα πνευματικά δικαιώματα είναι δικαιώματα πνευματικής ιδιοκτησίας και συνιστούν αποκλειστικά δικαιώματα που μπορούν να κατοχυρωθούν και να δώσουν τη δυνατότητα στο φορέα εκμετάλλευσης να αναζητήσει τρόπους προστασίας στις επενδύσεις του για να αναπτύξει ένα προϊόν, μια επωνυμία ή ένα σχέδιο. Ένα κατ' αποκλειστικότητα δικαίωμα δίνει στον κάτοχο τη δυνατότητα να παρεμποδίσει άλλους να κάνουν χρήση ενός προστατευμένου σήματος, μίας εφεύρεσης ή ενός σχεδίου. Το άτομο που είναι κάτοχος του αποκλειστικού δικαιώματος είναι επίσης σε θέσει να παρέχει χορηγήσεις αναφορικά με την αξιοποίηση των άυλων περιουσιακών στοιχείων του με αποζημίωση. Τα πιο σημαντικά δικαιώματα βιομηχανικής ιδιοκτησίας είναι τα διπλώματα ευρεσιτεχνίας, τα υποδείγματα χρησιμότητας, τα εμπορικά σήματα και τα δικαιώματα σχεδίασης. Σε πολλές χώρες, τα αντίστοιχα υπουργεία οικονομικών υποθέσεων και απασχόλησης είναι τα αρμόδια για τη θέσπιση νομοθεσίας αναφορικά με τα δικαιώματα βιομηχανικής ιδιοκτησίας και λαμβάνουν μέρος στις εργασίες που αφορούν τα

δικαιώματα βιομηχανικής ιδιοκτησίας στην ΕΕ αλλά και άλλα διεθνή φόρουμ (Löytömäki, 2021).

Β) Παραβιάσεις εργασιακής νομοθεσίας

Παρακάτω θα αναλυθεί η περίπτωση που οι εργοδότες προβούν σε παραβίαση της εργατικής νομοθεσίας; Το εργατικό δίκαιο είναι ένα από τα πιο ακανθώδη ζητήματα με τα οποία πρέπει οι εργοδότες να συμμορφώνονται. Ειδικότερα, οι πιο πολλές επιχειρήσεις υπόκεινται σε μια σειρά κανονιστικών και νομικών απαιτήσεων ομοσπονδιακά, πολιτειακά και τοπικά. Σωρευτικά, αυτοί οι κανονισμοί έχουν στόχο να προστατεύσουν τους εργαζόμενους. Για παράδειγμα, ο νόμος περί πολιτικών δικαιωμάτων του 1964 προστάτευε τους εργαζομένους από διακρίσεις, ενώ αντιθέτως ο νόμος περί δίκαιων προτύπων εργασίας (FLSA) του 1938 καθιέρωνε έναν ομοσπονδιακό κατώτατο μισθό και υπερωρίες για συγκεκριμένους υπαλλήλους. Το εργατικό δίκαιο κάνει αναφορά στο σύνολο των κανονισμών του είδους αυτού. Η κυβέρνηση λαμβάνει σοβαρά υπόψη τους συγκεκριμένους νόμους, ανεξάρτητα από το πόσο επαχθείς ή δύσκολοι μπορεί να είναι για τους εργοδότες, και η μη συμμόρφωση μπορεί να έχει πολλές σοβαρές συνέπειες (Coadvantage.com, χ.χ.).

Σημαντικό είναι και το ερώτημα που προκύπτει που αφορά τους κινδύνους που θα πρέπει να αντιμετωπίσουν οι εργοδότες που προβαίνουν σε παραβίαση της εργατικής νομοθεσίας. Η ανάλυση αφορά οικονομικές κυρώσεις, νομικές δαπάνες, δυσμενείς νομικές αποφάσεις που μπορεί να καταλήξουν και στο κλείσιμο μίας επιχείρησης και προβλήματα φήμης (Coadvantage.com, χ.χ.).

Οικονομικές κυρώσεις

Η πλειοψηφία των εργατικών νόμων επιτρέπουν κυρώσεις. Για παράδειγμα, σύμφωνα με το Υπουργείο Εργασίας, οι εργοδότες που παραβιάζουν ηθελημένα τους νόμους για τον κατώτατο μισθό είναι πιθανό να ενδέχεται να υφίστανται αστική ποινή για την κάθε παραβίαση. Οι παραβιάσεις που σχετίζονται με την προστασία της παιδικής εργασίας έχουν αστική ποινή για την κάθε παραβίαση. Σύμφωνα με τη συγκεκριμένη απαίτηση για συμμόρφωση, οι εργαζόμενοι είναι πιθανό να έχουν δικαίωμα σε αποδοχές που είναι καθυστερημένες, την αξία των παροχών που έχουν χαθεί και πληρωμές τόκων (Coadvantage.com, χ.χ.).

Νομικές δαπάνες

Επιπλέον, οι παραβιάσεις της εργατικής νομοθεσίας μπορεί να προσφέρουν λόγους στους εργαζόμενους να υποβάλουν ιδιωτικές αγωγές κατά του εργοδότη, πράγμα που σημαίνει ότι ο εργοδότης μπορεί να είναι υπεύθυνος για νομικές αμοιβές και, εάν χαθεί η υπόθεση θα πρέπει να καταβάλλει ένα ποσό αποζημίωσης. Σε μια περίπτωση, η «αδυναμία

του εργοδότη να διατηρήσει ακριβή αρχεία χρόνου» μπορεί να οδηγήσει σε νομικές δαπάνες για ενόρκους ύψους 5,8 εκατομμυρίων δολαρίων στις ΗΠΑ που επικυρώθηκε από το Ανώτατο Δικαστήριο, σύμφωνα με την Εταιρεία Διαχείρισης Ανθρώπινου Δυναμικού (Coadvantage.com, χ.χ.).

Δυσμενείς νομικές αποφάσεις

Εκτός από τα δικαστικά έξοδα, τα τέλη διακανονισμού ή τις αμοιβές των ενόρκων, οι διαφορές που προκύπτουν από παραβιάσεις της εργατικής νομοθεσίας μπορεί να έχουν άλλες νομικές συνέπειες για τους εργοδότες. Για παράδειγμα, το 2018 το Εθνικό Συμβούλιο Εργασιακών Σχέσεων (NLRB) προέτρεψε τα περιφερειακά γραφεία να «επιδιώξουν πιο επιθετικά τις προσωρινές διαταγές για να σταματήσουν κατηγορίες δυνητικά αθέμιτων εργασιακών πρακτικών». Δηλαδή, τα νομικά ευρήματα μπορούν να προβούν σε παραβίαση της ικανότητας του εργοδότη να εξασκεί τις δραστηριότητές του με κανονικό τρόπο. Σε ακραίες περιπτώσεις, τα δικαστήρια μπορούν ακόμη και να κλείσουν τις επιχειρήσεις (Coadvantage.com, χ.χ.).

Προβλήματα φήμης

Κάποιες παραβιάσεις που αφορούν το εργατικό δίκαιο μπορούν ακόμη και να έλξουν την προσοχή των μέσων μαζικής ενημέρωσης και να ωθήσουν σε αύξηση του δημόσιου ελέγχου της επιχειρηματικής συμπεριφοράς. Για παράδειγμα, κυκλοφόρησε η είδηση από την εταιρεία Starbucks μετά από παράπονα για ορισμένες από τις εργασιακές της πρακτικές. Ο αντίκτυπος αυτής της κάλυψης από τα μέσα μπορεί να παρουσιάζει ποικιλία σε ευρύ φάσμα, αλλά κανένας εργοδότης δεν επιθυμεί να αντιμετωπίσει κρίση δημοσίων σχέσεων που θα μπορούσε πιθανόν να προκαλέσει διαταραχές στις επιχειρήσεις και να συνεισφέρει στο να αποθαρρυνθούν οι πελάτες (Coadvantage.com, χ.χ.).

Γ) Παραβιάσεις αντιμονοπωλιακών νόμων

Οι αντιμονοπωλιακές νομοθεσίες έχουν σκοπό να προστατεύσουν τον ανταγωνισμό στην αγορά. Ο ανταγωνισμός λογίζεται ευεργετικός εφόσον συνεισφέρει στην εξοικονόμηση χρημάτων από τους καταναλωτές και παρέχει ενθάρρυνση στις επιχειρήσεις να παράγουν καλύτερα ποιοτικά προϊόντα. Σε μια αγορά που είναι ανταγωνιστική, οι εταιρείες πρέπει να χρεώσουν πιο χαμηλά ή να προσφέρουν προϊόντα με πιο υψηλή ποιότητα ώστε να κερδίσουν με επιτυχία τις επιχειρήσεις των καταναλωτών. Η αντιμονοπωλιακή νομοθεσία αποσκοπεί στη διατήρηση του ανταγωνισμού προκειμένου να προωθήσει αυτές τις ωφέλειες για τους καταναλωτές. Οι παραβιάσεις θεωρούνται ένα είδος εγκλήματος των στελεχών μίας επιχείρησης επειδή βλάπτουν τον ανταγωνισμό, προκαλούν αύξηση των

τιμών για τον τελικό καταναλωτή και μπορούν ενδεχομένως να βλάψουν την οικονομία (No author, 2021).

Δ) Παραβιάσεις εμπορικής νομοθεσίας και αθέμιτου ανταγωνισμού

Οι νόμοι περί αθέμιτου ανταγωνισμού έχουν σχεδιαστεί για να προστατεύουν τους καταναλωτές και τις επιχειρήσεις από παραπλανητικές επιχειρηματικές πρακτικές. Μερικά κοινά παραδείγματα αθέμιτων ανταγωνιστικών πρακτικών στο εμπορικό δίκαιο περιλαμβάνουν: παραβιάσεις εμπορικών σημάτων, εμπορική δυσφήμιση και κατάχρηση επιχειρηματικών εμπορικών μυστικών. Όσον αφορά τους καταναλωτές, οι νόμοι περί αθέμιτου ανταγωνισμού συνήθως αποτρέπουν τις αθέμιτες στρατηγικές τιμολόγησης, όπως η πλαστογραφία και οι ψευδείς ή παραπλανητικές δηλώσεις (Hg.org, 2021).

Παραβίαση εμπορικού σήματος

Μια κοινή μορφή αθέμιτου ανταγωνισμού είναι η παραβίαση των αποκλειστικών δικαιωμάτων που συνδέονται με ένα εμπορικό σήμα χωρίς την άδεια του κατόχου του εμπορικού σήματος. Η παραβίαση μπορεί να λάβει χώρα όταν ένα μέρος, για παράδειγμα ο "παραβάτης", χρησιμοποιεί ένα εμπορικό σήμα που δεν διακρίνεται ή είναι εκπληκτικά παρόμοιο με ένα εμπορικό σήμα που ανήκει σε άλλο μέρος, σε σχέση με προϊόντα ή υπηρεσίες που είναι πανομοιότυπα ή παρόμοια με τα προϊόντα ή τις υπηρεσίες που καλύπτει η καταχώριση. Ο κάτοχος του εμπορικού σήματος μπορεί να κινήσει αστικές νομικές διαδικασίες κατά του παραβάτη και, σύμφωνα με τον νόμο περί παραποίησης εμπορικών σημάτων του 1984, ορισμένες πράξεις παραβίασης εμπορικού σήματος μπορεί ακόμη και να τιμωρηθούν ως έγκλημα. Συνήθη παραδείγματα παραβίασης εμπορικών σημάτων περιλαμβάνουν προϊόντα απομίμησης, όπως τσάντες χειριού, ρολόγια και ταινίες που έχουν παραδοθεί (Hg.org, 2021).

Εμπορική δυσφήμιση

Η εμπορική δυσφήμιση είναι μια σκόπιμη, ψευδής επικοινωνία, γραπτή ή προφορική, που βλάπτει τη φήμη μιας επιχείρησης/ατόμου. Αυτή η ψευδής επικοινωνία πρέπει να μειώνει τον σεβασμό, τον σεβασμό ή την εμπιστοσύνη στην οποία διατηρείται η επιχείρηση ή το άτομο ή να προκαλεί απαξιωτικές, εχθρικές ή δυσάρεστες απόψεις ή συναισθήματα εναντίον της επιχείρησης ή του ατόμου. Ενώ όσο πιο έντονη είναι η εμπορική δυσφήμιση είναι αστική υπόθεση, σε λίγες περιπτώσεις μπορεί να γίνει ποινική. Η εμπορική δυσφήμιση μπορεί επίσης να περιλαμβάνει τόσο γραπτές δηλώσεις, γνωστές ως συκοφαντία, όσο και προφορικές δηλώσεις, που ονομάζονται συκοφαντία. Εάν έχετε ερωτήσεις σχετικά με τον αθέμιτο ανταγωνισμό, μπορείτε να χρησιμοποιήσετε τους πόρους που βρίσκονται παρακάτω για να ερευνήσετε περαιτέρω το θέμα (hg.org, 2021).

Ε) παραβίαση νομοθεσίας περί των εκπτώσεων.

Στην Ελλάδα ο νόμος 4177-13 με τίτλο «Κανόνες ρύθμισης της αγοράς προϊόντων και της παροχής υπηρεσιών» ανάμεσα σε άλλα ορίζει το τι πρέπει να πραχθεί αναφορικά με τις εκπτώσεις και τις προσφορές σε προϊόντα.
Ειδικότερα όσον αφορά τις εκπτώσεις – Προσφορές, ο νόμος όρισε ότι είναι επιτρεπτό να πωλούνται εμπορεύματα ή να παρέχονται υπηρεσίες με ελαττωμένες τιμές τέσσερις φορές κατά τη διάρκεια ενός έτους. Πιο συγκεκριμένα προσδιορίζονται τα εξής:
Α) Τακτικές εκπτώσεις σε συγκεκριμένες ημερομηνίες όπως είναι η δεύτερη Δευτέρα του Ιανουαρίου μέχρι και το τέλος Φεβρουαρίου κα η δεύτερη Δευτέρα του Ιουλίου μέχρι το τέλος Αυγούστου.

β) Ενδιάμεσες περίοδοι που λαμβάνουν χώρα εκπτώσεις όπως το πρώτο δεκαήμερο του Μαΐου και το πρώτο δεκαήμερο του Νοεμβρίου.
Η συγκεκριμένη διάταξη δεν αφορά πωλήσεις αυτοκινήτων.
Επιπρόσθετα σε διάστημα τριάντα ημερών από την απαρχή των εκπτώσεων δεν επιτρέπεται στους υπεύθυνους των εμπορικών καταστημάτων να προβούν σε ανακοίνωση προς το κοινό εκπτώσεων καθ' οιανδήποτε τρόπο, ειδικότερα μέσω διαφήμισης, επιστολών ή αναρτήσεων διαφημιστικών πινακίδων.

Σύμφωνα με τα όσα ορίζονται στην παραπάνω παράγραφο κατά τη διάρκεια των εκπτώσεων εκτός από την αναγραφή της προ εκπτώσεων τιμής αλλά και της νέας θα πρέπει να αναγράφεται και το ποσοστό της έκπτωσης. Στην περίπτωση που λαμβάνει χώρα περίοδος προσφορών είναι επιτρεπτό κατ' αποκλειστικό να αναγράφεται η προηγούμενη τιμή και η νέα δίχως το ποσοστό (Ν. 4177/13, ΦΕΚ 173 Α/8-8-2013).
Οι προσφορές συγκεκριμένων προϊόντων είναι επιτρεπτές για χρονικό διάστημα που δεν μπορεί να ξεπερνά τις δέκα (10) συνεχόμενες ημέρες, εφόσον αναγράφονται με ευκρίνεια η προηγούμενη και η καινούργια τιμή των προϊόντων σε εμφανή σημεία του καταστήματος και οπωσδήποτε στα σημεία όπου εκτίθενται τα προσφερόμενα προϊόντα. Κατ' εξαίρεση, ο χρόνος των προσφορών από εκθέσεις αυτοκινήτων δεν μπορεί να υπερβεί τις εξήντα (60) ημέρες. Η συγκεκριμένη διάταξη δεν τίθεται σε εφαρμογή στις προσφορές προϊόντων παντοπωλείου (Ν. 4177/13, ΦΕΚ 173 Α/8-8-2013).

Επιπρόσθετα, είναι απαγορευτική η προσφορά ειδών, των οποίων η ποσότητα υπερβαίνει το πενήντα τοις εκατό (50%) του συνόλου των ειδών που διατίθενται από το κατάστημα. Ως είδος, ορίζεται ο κάθε κωδικός προϊόντος τον οποίο πουλά η επιχείρηση.
Νέα προσφορά του ίδιου προϊόντος δεν είναι επιτρεπτή να τεθεί αν δεν παρέλθει διάστημα εξήντα (60) ημερών από την προηγούμενη.
Ο υπεύθυνος κάθε εμπορικού καταστήματος θα πρέπει να προβεί στην ανακοίνωση μέσω ηλεκτρονικής αλληλογραφίας (e-mail) ή τηλεμοιότυπου (σπανιότερα στη σημερινή εποχή)

στο Παρατηρητήριο Τιμών της Γενικής Γραμματείας Καταναλωτή του Υπουργείου Ανάπτυξης και Ανταγωνιστικότητας τις προσφορές που έχει την πρόθεση να κάνει, τουλάχιστον μία (1) ημέρα προτού αρχίσει η εφαρμογή τους. Στην ανακοίνωση θα πρέπει να γίνεται αναφορά στα προϊόντα που προσφέρονται και για πόσο χρονικό διάστημα θα είναι σε ισχύ η προσφορά. Την ίδια ανακοίνωση θα πρέπει να αναρτήσει στην ιστοσελίδα του καταστήματος στο διαδίκτυο (αν υπάρχει) και θα πρέπει η ίδια ανακοίνωση να κοινοποιηθεί με κάθε πρόσφορο τρόπο στον οικείο Εμπορικό Σύλλογο (Ν. 4177/13 (ΦΕΚ 173 Α/8-8-2013).
Τέλος, κατόπιν απόφασης του Υπουργού Ανάπτυξης και Ανταγωνιστικότητας που ήταν αρμόδιος τη χρονική στιγμή που εξεδόθη ο συγκεκριμένος νόμος, καθόρισε και τη χρονική περίοδο που τα εποχικά είδη μπορούν να παρέχονται με μειωμένη τιμή. Παρομοίως, με ίδια απόφαση καθορίστηκαν οι όροι και οι προϋποθέσεις για να πραγματοποιηθεί ο χαρακτηρισμός ενός καταστήματος που πουλά αποθέματα (stock) αλλά και κατάστημα που λογίζεται εκπτωτικό (outlet), καθώς και ο τρόπος που θα πουλούνται τα εμπορεύματα από τα συγκεκριμένα καταστήματα (Ν. 4177/13, ΦΕΚ 173 Α/8-8-2013).

Εκτός από τις παραπάνω το 1980-1990 αξίζει να σημειωθεί ότι εκείνη την περίοδο οι φαρμακευτικές εταιρείες, διύλισης πετρελαίου και κατασκευής αυτοκίνητων ήταν υπεύθυνες για τις μισές από τις παραβάσεις που καταγράφηκαν και το 80% ήταν μεσαίας ή σοβαρής σπουδαιότητας.(Τσουραμάνης ,1996)

Επιπλέον οι παραπάνω μέσω ελέγχων που διενήργησαν επίσης ότι παραβίαζαν τους κανόνες προστασίας του περιβάλλοντος και επιπρόσθετα υπήρξε δωροδοκία πολίτικων προσώπων για να ευνοηθούν οι παραβιάσεις των κανόνων ισοτιμίας . Συμπληρωματικά η παραβίαση κανόνα παραγωγής ειδικότερα για τις βιομηχανίες αυτοκινήτων για ελλαττωματικά οχήματα όπως το diesel gate της αυτοκινητοβιομηχανίας Volkswagen μεταξύ 2017-2018.

Πέρα από αυτό, η παραβίαση κανόνων διαχείρισης και τα σφάλματα στα εμπορεύματα ή ακατάλληλες συνθήκες φύλαξης ή παραγωγής (Ε.Φ.Ε.Τ ,2021)

Οι επιχειρήσεις έχουν και επίσης σύμφωνα με τον Walton και Yeager έχουν και ηθικές παρεκκλίσεις οι οποίες ακολουθούνται και αρκετά συχνά . Μερικές από αυτές είναι. κυρίως μέσω από τα ΜΜΕ μέσω των διαφημίσεων που παρουσιάζουν τις διάφορες επιχειρήσεις μοναδικές στο είδος τους .

Επίσης, μέσω της τηλεόρασης και του ραδιοφώνου δείχνοντας προς τα έξω μια εικόνα εξαιρετικά φιλική προς τους πολίτες.

Εν τέλει, ο αθέμιτος ανταγωνισμός και η κατασκόπευση και η εξαγορά διαφόρων πρωτοτύπων ιδεών από διαφόρους υπαλλήλους. (Τσουραμάνης . 1996)

1.2.2 Η ΦΟΡΟΔΙΑΦΥΓΗ

Η **φοροδιαφυγή** είναι *« Κατά τον Κούλη, η παράνομη αποφυγή της φορολογικής υποχρέωσης , η οποία αφορά όλους τους φόρους τόσο τους αμέσους , όσο και τους έμμεσους. Ανάλογα με το είδος του φόρου είναι και ο τρόπος πραγματοποίησης της.»(Κούλης ,1970)*

Στην Ελλάδα τα τελευταία χρόνια το ποσοστό κυμαίνεται μεταξύ 6% και 9% του συνολικού ΑΕΠ κάθε χρόνο δηλαδή περίπου χρέος στο δημόσιο περίπου 11- 16 δισεκατομμύρια ευρώ που αυτό προσμετράτε στο δημόσιο χρόνιο έλλειμα που διαθέτει η χωρά μας με αποτέλεσμα την αύξηση των φορολογικών συντελεστών για την κάλυψη αυτών των ελλειμάτων. (Γεωργακόπουλος 2016)

Συνήθως αυτοί που φοροδιαφεύγουν στην χώρα μας είναι κυρίως οι αυτοαπασχολούμενοι και οι μικρές επιχειρήσεις. Αυτό παρόλα αυτά συμβαίνει και σε άλλες ευρωπαϊκές χώρες αλλά και στις Ηνωμένες Πολιτείες. Βέβαια εκεί συμβαίνει και κάτι άλλο. Εκεί χωρίζουμε σε μικρούς και μεγάλους. Στους μικρούς ανήκουν τα παραπάνω που αναφέραμε. Στους μεγάλους ανήκουν οι μεγάλο- εταιρίες οι οποίες κάνουν και μεγάλες εξαγωγές , οι τουριστικές επιχειρήσεις καθώς και οι εταιρίες πετρελαίων. Όμως οι μικρές επιχειρήσεις δεν προκαλούν τόσο μεγάλο πρόβλημα ειδικά στην Ευρώπη καθώς και οι αυτό απασχολούμενοι διότι στην πλειοψηφία δεν επικρατεί αυτά τα είδη απασχόλησης. (Γεωργακόπουλος, 2016)

Παρόλα αυτά η Ελλάδα διατηρεί πολύ ψηλά τα ποσοστά της σε αυτές του είδους εργασίες σε σχέση με την υπόλοιπη Ευρώπη (συγκεκριμένα κατά 34 % υψηλότερη οι αυτοαπασχολούμενοι και κατά 59 % υψηλότερη η ανάπτυξη των μικρών επιχειρήσεων) (Eurostat 2012).

Οι τρόποι με τους οποίους όλες οι παραπάνω επιχειρήσεις μπορούν να φοροδιαφύγουν είναι μερικές από τι παρακάτω:

α) η μη έκδοση τιμολογίων- αποδείξεων και δελτίων αποστολής έτσι ώστε να δείχνουν μικρό τζίρο

β) η χρήση εικονικών τιμολογίων για την αύξηση των δαπανών των επιχειρήσεων. Με αυτόν τον τρόπο μειώνουν τα κέρδη και έτσι μειώνεται το ποσό καταβολής ΦΠΑ

γ) η χρησιμοποίηση πολλών διαφορετικών ΑΦΜ (Αριθμών Φορολογικού Μητρώου)

δ) η εισαγωγή προϊόντων που δεν δηλώνονται καθόλου ή εικονίζονται ως κάποιου άλλου είδους προϊόντα.

Ε) η απόκρυψη περιουσιακών στοιχείων και άλλων τεκμαρτών εισοδημάτων που προέρχονται από αυτά

ΣΤ) οι διαφορές ανάμεσα στις εκκαθαριστικές και στις προσωρινές δηλώσεις του ΦΠΑ.

Συμπληρωματικά όμως , μπορούμε να αναφέρουμε και τους λόγους που συντελούν στην ανάπτυξη της φοροδιαφυγής :

Α) το ύψος της φορολογικής επιβάρυνσης. Συγκεκριμένα όταν η επιβάρυνση είναι υψηλή η φοροδιαφυγή θεωρείται ένα μέσο άμυνας για την αποσυμπίεση των χρεών των φορολογουμένων επιχειρήσεων.

Β) η ανύπαρκτη πολιτική βούληση για την μείωση των φόρων δηλαδή ανύπαρκτη μελέτη από ηγετικά στελέχη του κράτους για την φοροελάφρυνση τόσο των πολίτων όσο και στις επιχειρήσεις (Γεωργακόπουλος 2016).

Γ) η πιθανότητα εντοπισμού από ελεγκτικούς φορείς του κράτους. Γι' αυτό οι έλεγχοι θα πρέπει να είναι εντατικότεροι και οι ποινές πολύ αυστηρότερες σε σχέση με την εκάστοτε νομοθεσία.

Ο Αμερικανός δικαστής Όλιβερ Γουέντελ Χολμς υποστήριξε ότι οι φόροι αποτελούν το αντίτιμο που ο κόσμος πληρώνει για να ζήσει σε μια πολιτισμένη κοινωνία. Σε μία έρευνα που διενεργήθηκε πρόσφατα από την εταιρεία ερευνών ΔιαΝΕΟσις οι ερωτηθέντες έδειξαν να συμφωνούν: 85,5% υποστήριξαν πως λογίζου τη φοροδιαφυγή κλοπή. Την ίδια στιγμή, το 35,1% υποστήριξε πως πολύ ευχάριστα προβαίνει σε πράξεις φοροδιαφυγής όταν δίνεται η ευκαιρία καθώς γίνεται από την πλειοψηφία (Γεωργακόπουλος, 2016).

Το πρόβλημα της φοροδιαφυγής λογίζεται ως ένα από τα πιο σημαντικά προβλήματα που πρέπει να αντιμετωπιστεί από ένα κράτος. Στην Ελλάδα διαφαίνεται ότι το συγκεκριμένο πρόβλημα είναι ιδιαίτερα έντονο. Σύμφωνα με μελέτες η φοροδιαφυγή στην Ελλάδα είναι πιο μεγάλη από ό,τι σε άλλες ανεπτυγμένες χώρες, πράγμα που δυσχεραίνει ακόμα περισσότερο την κατάσταση ειδικά όταν η Ελλάδα βρισκόταν σε άσχημη θέση λόγω της παγκόσμιας κρίσης (Γεωργακόπουλος, 2016).

1.2.3 Πόση είναι η φοροδιαφυγή στην Ελλάδα;

Προφανώς, δεν είναι εφικτό να είναι γνωστό επακριβώς το μέγεθος της φοροδιαφυγής στην Ελλάδα. Μπορεί να εκτιμηθεί ωστόσο και τέτοιες εκτιμήσεις έχουν πραγματοποιηθεί μέσω ερευνών που προσμετρούν σε ενδεικτικό βαθμό το μέγεθος όχι όμως την ίδια. Έτσι σύμφωνα με τις έρευνες:

Τα διαφυγόντα έσοδα από τη φοροδιαφυγή των **φυσικών προσώπων** είναι **από 1,9% ως 4,7% του ΑΕΠ** σε ετήσια βάση.

Από τη φοροδιαφυγή στον **ΦΠΑ** εκτιμάται ότι υπάρχει απώλεια του **3,5% του ΑΕΠ**.

Οι απώλειες από το **λαθρεμπόριο** ποτών, τσιγάρων και καυσίμων είναι αντίστοιχες σε περίπου **0,5% του ΑΕΠ**.

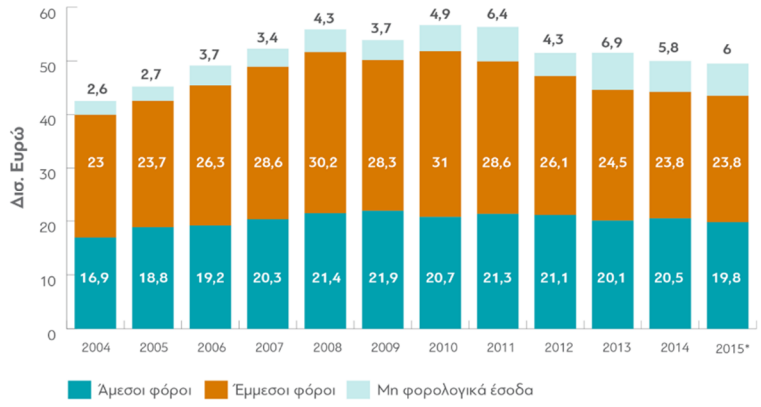
Για τα νομικά πρόσωπα, τα διαφυγόντα κέρδη για τη χώρα από τη φοροδιαφυγή και φοροαποφυγή των **επιχειρήσεων** εκτιμώνται περίπου στο **0,15% του ΑΕΠ**.

Κατά συνέπεια, το μέγεθος της φοροδιαφυγής στην Ελλάδα υπολογίζεται **από 6% ως 9% του ΑΕΠ**, δηλαδή **ανάμεσα σε €11 και €16 δισ. το χρόνο**.

Ποιος πληρώνει φόρους στην Ελλάδα;

Το ελληνικό κράτος έχει καταγράψει **έσοδα ύψους περίπου €50 δισεκατομμυρίων σε ετήσια βάση**. Αυτά είναι τα έσοδα, με αυτά και με τις ασφαλιστικές εισφορές και τα δάνεια των μνημονίων πρέπει να καλύπτονται όλα του τα έξοδα για τη λειτουργία του, για την αποπληρωμή δανείων (περίπου **€12 δισ.** το χρόνο), για την πληρωμή συντάξεων (**€28 δισ.** το χρόνο), για τους μισθούς των δημοσίων υπαλλήλων (περίπου **€15 δισ.** το χρόνο) και, σύμφωνα με τα μνημόνια που έχει υπογράψει με τους δανειστές του, από αυτά πρέπει να εξασφαλίσει και σημαντικά πρωτογενή πλεονάσματα τα επόμενα χρόνια (Γεωργακόπουλος, 2016).

Έσοδα Τακτικού Προϋπολογισμού

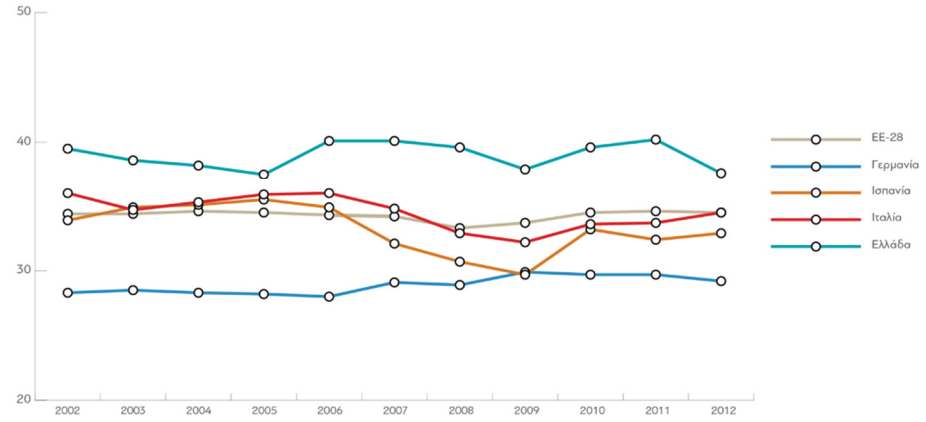


Πηγή: Έκθεση του Διοικητή της Τράπεζας της Ελλάδος * Προσωρινά στοιχεία

Σύμφωνα με τα τελευταία στοιχεία για το 2015, το 88% αυτών των εσόδων του κεντρικού κράτους (δεν περιλαμβάνουν τις ασφαλιστικές εισφορές που εισπράττουν τα ταμεία) προέρχονται από τη φορολογία, και τα υπόλοιπα από άλλες πηγές, συμπεριλαμβανομένων των αποκρατικοποιήσεων. Από τα φορολογικά έσοδα, οι άμεσοι φόροι φέρνουν **περίπου €20 δισ.**, ενώ οι έμμεσοι (ΦΠΑ, φόροι καυσίμων, καπνών κλπ) φέρνουν **περίπου €24 δισ**. Αυτό είναι ένα σημαντικό δεδομένο. Είναι γνωστό ότι οι έμμεσοι φόροι είναι πιο "άδικοι" καθώς πλήττουν με τον ίδιο τρόπο και τους πλούσιους και φτωχούς. Τα φορολογικά συστήματα των πιο πολλών από τις ανεπτυγμένες χώρες στηρίζονται βασίζονται κατά το πλείστο σε άμεσους φόρους παρά σε έμμεσους. Στους έμμεσους φόρους στηρίζονται περισσότερο φορολογικά συστήματα αναπτυσσόμενων ή τριτοκοσμικών χωρών (Γεωργακόπουλος, 2016).

Φορολογικά Έσοδα ως % του ΑΕΠ & Έμμεσοι Φόροι ως Ποσοστό (%) των Συνολικών Φόρων

Έμμεσοι Φόροι ως Ποσοστό των συνολικών φόρων (%)

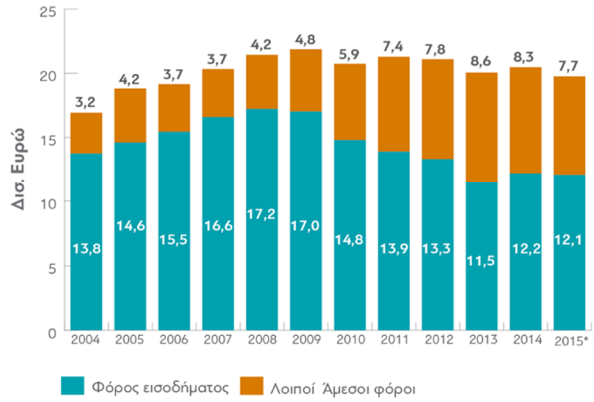


Πηγή: ΟΟΣΑ, EU DG Taxation and Customs Union, Eurostat

Όπως διαφαίνεται στον παραπάνω πίνακα, τα έσοδα της χώρας ελαττώθηκαν σε σταθερή βάση από το 2010 και μετά, με τη μεγαλύτερη ελάττωση να διαφαίνεται στους έμμεσους φόρους. Στους άμεσους, ελαττώθηκαν με ραγδαίο ρυθμό οι εισπράξεις από το φόρο εισοδήματος (από 17,2 δισεκατομμύρια το 2008 σε 12,1 το 2015) κάτι που ήταν προσδοκώμενο, καθώς ελαττώθηκαν με ραγδαίο ρυθμό και τα εισοδήματα των πολιτών. Την ίδια στιγμή, όμως, μέσα στην κρίση σημείωσαν θεαματική άνοδο οι υπόλοιποι άμεσοι φόροι, ενώ υπήρξαν και νέοι (εισφορά αλληλεγγύης, ΕΝΦΙΑ) που συνέβαλλαν στο να ελαττωθούν τα έσοδα άμεσων φόρων για το κράτος (Γεωργακόπουλος, 2016).

Άμεσοι Φόροι

Άμεσοι Φόροι – Φόρος Εισοδήματος & Λοιποί Άμεσοι Φόροι (Δισ. Ευρώ)



Πηγή: Έκθεση του Διοικητή της Τράπεζας της Ελλάδος * Προσωρινά στοιχεία

Μέσα στην κρίση, οι πολίτες πληρώνουν πάνω-κάτω τους ίδιους άμεσους φόρους που πλήρωναν και πριν, παρ' όλο που έχουν πολύ χαμηλότερα εισοδήματα από πριν. Από ό,τι φαίνεται, μέχρι και τα πρώτα χρόνια της κρίσης τους φόρους τους πλήρωναν μερικοί από αυτούς που θα αποκαλούσαμε "πλούσιους". Στην Ελλάδα το 2011 που ήταν και η τελευταία χρονιά για την οποία υπήρχαν αναλυτικά επίσημα στοιχεία από τη ΓΓΠΣ. Αξίζει να τονιστεί πως η υποβολή των φορολογικών δηλώσεων αναλογούσε στα **5,7 εκατομμύρια**, ένας αριθμός που έχει παραμείνει σταθερός τα τελευταία δέκα χρόνια. Περίπου οι μισές από αυτές (**49%**) σχετίζονταν με εισοδήματα **κάτω των €12.000**. Οι αυτοαπασχολούμενοι, δε, δήλωναν εισοδήματα κάτω από το τότε αφορολόγητο όριο των €12.000 σε ποσοστό **64%** (δήλωναν μέσο όρο εισοδημάτων 4.300 ο καθένας). Όλοι αυτοί οι φορολογούμενοι κατέβαλλαν **λιγότερο από το 1%** του συνόλου των φορολογικών εσόδων. Με άλλα λόγια, **2,8 εκατομμύρια πολίτες** πλήρωσαν φόρο συνολικά **60 εκατομμύρια ευρώ**, δηλαδή **€21,4 ο καθένας**. Εν αντιθέσει, το **8%** των φορολογούμενων που δήλωσαν εισοδήματα άνω των €42.000 σε ετήσια βάση, περίπου 400.000 πολίτες, πλήρωσαν **το 69% των φόρων** εισοδήματος φυσικών προσώπων (Γεωργακόπουλος, 2016).

Στοιχεία για τη Φορολογική Βάση των Φυσικών Προσώπων ανά Κατηγορία Εισοδήματος

		2006	2007	2008	2009	2010	2011
ΦΠ με Εισόδημα < €12.000	Αριθμός φορολογικών δηλώσεων (εκατομμύρια)	3,1	3,0	2,9	2,8	2,8	2,8
	% του συνόλου	57%	54%	51%	49%	49%	49%
	Εισόδημα (εκατομμύρια €)	18,404	18,047	17,398	16,479	15,841	15,294
	% του συνόλου	23%	21%	19%	17%	16%	16%
	Συνολικός φόρος (εκατομμύρια €)	33	33	23	23	24	60
	% του συνόλου	0,5%	0,4%	0,3%	0,3%	0,3%	0,8%
ΦΠ με Εισόδημα από €12.000 έως €42.000	Αριθμός φορολογικών δηλώσεων (εκατομμύρια)	2,1	2,2	2,4	2,4	2,4	2,4
	% του συνόλου	38%	40%	42%	43%	43%	43%
	Εισόδημα (εκατομμύρια €)	44,084	46,924	50,512	52,568	53,188	53,421
	% του συνόλου	55%	55%	54%	54%	53%	55%
	Συνολικός φόρος (εκατομμύρια €)	3,365	3,681	3,606	3,610	3,463	2,241
	% του συνόλου	46%	44%	41%	40%	38%	31%
ΦΠ με Εισόδημα > €42.000	Αριθμός φορολογικών δηλώσεων (εκατομμύρια)	0,3	0,3	0,4	0,5	0,5	0,4
	% του συνόλου	5%	6%	7%	8%	9%	8%
	Εισόδημα (εκατομμύρια €)	18,070	21,035	25,414	29,014	31,272	29,230
	% του συνόλου	22%	24%	27%	30%	31%	30%
	Συνολικός φόρος (εκατομμύρια €)	3,937	4,604	5,123	5,489	5,527	5,036
	% του συνόλου	54%	55%	59%	60%	61%	69%

Πηγή: Στατιστικό Δελτίο Φορολογικών Δεδομένων (2006-2011 Οικ.Έτη), ΓΓΠΣ

Παρόμοια είναι η εικόνα και στις επιχειρήσεις. Στην Ελλάδα το 2011 υπήρχαν **220.000 επιχειρήσεις** που δήλωναν ετήσια κέρδη λιγότερα από 1,2 εκατομμύρια ευρώ, και **μόλις 901 επιχειρήσεις** που δήλωναν περισσότερα κέρδη. Οι δεύτερες, που αποτελούν **το 0,4%** των ελληνικών επιχειρήσεων και κατέβαλλαν **το 61%** των φόρων.

Οι πρώτες πλήρωναν φόρο κατά μέσο όρο **€5.400** ετησίως. Οι δεύτερες πλήρωναν φόρο κατά μέσο όρο **€2,1 εκ.** ετησίως.

		2006	2007	2008	2009	2010	2011
Με Κέρδη < €1.200.000	Πλήθος επιχειρήσεων	190.839	202.767	212.115	220.131	223.989	220.137
	% του συνόλου	99,5%	99,4%	99,4%	99,4%	99,5%	99,6%
	Φορολογητέα κέρδη (εκατομμύρια €)	4.817	5.313	6.037	6.006	5.469	5.018
	% του συνόλου	33%	31%	31%	36%	36%	39%
	Κύριος και Συμπληρωματικός φόρος (εκατομμύρια €)	1.403	1.411	1.414	1.400	1.276	1.186
	% του συνόλου	32%	30%	30%	34%	35%	39%
Με Κέρδη > €1.200.000	Πλήθος επιχειρήσεων	969	1.132	1.353	1.232	1.101	901
	% του συνόλου	0,5%	0,6%	0,6%	0,6%	0,5%	0,4%
	Φορολογητέα κέρδη (εκατομμύρια €)	9.610	11.677	13.366	10.704	9.604	7.793
	% του συνόλου	67%	69%	69%	64%	64%	61%
	Κύριος και Συμπληρωματικός φόρος (εκατομμύρια €)	3.044	3.336	3.299	2.658	2.347	1.880
	% του συνόλου	68%	70%	70%	66%	65%	61%

Πηγή: Στατιστικό Δελτίο Φορολογικών Δεδομένων (2006-2011), ΓΓΠΣ

Δηλαδή, το 2011 το 8% των φορολογούμενων κατέθετε το 69% των φόρων φυσικών προσώπων, και το 0,4% των επιχειρήσεων πλήρωνε το 61% των φόρων νομικών προσώπων στη χώρα μας. Οι "πλούσιοι" ήταν αυτοί που σήκωναν το φορολογικό βάρος της χώρας. Και ποιοι είναι αυτοί οι "πλούσιοι"; Στη συντριπτική τους πλειοψηφία

υψηλόμισθοι μισθωτοί και **πολύ μεγάλες επιχειρήσεις**. Η μεγάλη πλειοψηφία των εσόδων από φόρους εισοδήματος προερχόταν από αυτούς. Σύμφωνα με τα ανεπίσημα στοιχεία που έχει στη διάθεσή της η διαΝΕΟσις -και που έχουν δημοσιευτεί κατά καιρούς και στον Τύπο- για το φορολογικό έτος 2014, υπάρχει μια **θεαματική μετατόπιση των εισοδημάτων προς τα κάτω** (τα φυσικά πρόσωπα που δηλώνουν έσοδα άνω των 42.000 δεν είναι πια το 8% - είναι μόνο το 1,6%) , και μια παράλληλη **μετατόπιση των φορολογικών βαρών στα μεσαία στρώματα** (Γεωργακόπουλος, 2016).

Συνολικό Δηλωθέν Εισόδημα ανά Κλίμακα και Επαγγελματική Κατηγορία (Φορολογικό Έτος 2014)

Κλιμάκιο Εισοδήματος (€)	Συνολικός Αριθμ. Φορολογουμένων (Εκατ.)	% του Συνόλου Φορολογουμένων	Συνολικό Δηλωθέν Εισόδημα (Δισ. €)	% του Συνόλου Εισοδημάτων	Συνολικός Φόρος (Δισ. €)	% του Συνολικού Φόρου
(0 - 12.000]	5.06	68.9%	22.97	31.1%	0.89	11.1%
(12.000 - 42.000]	2.16	29.5%	41.12	55.6%	4.79	59.5%
> 42.000	0.12	1.6%	9.84	13.3%	2.7	29.5%
Σύνολο	**7.34**	**100.0%**	**73.93**	**100.0%**	**8.6**	**100.0%**

	Μισθωτοί & Συνταξιούχοι		Ελεύθεροι Επαγγελματίες		Λοιποί	
Κλίμακα Εισοδήματος (€)	% του Συνόλου Αριθμού Φορολογουμένων	% του Συνόλου Εισοδημάτων	% του Συνόλου Αριθμού Φορολογουμένων	% του Συνόλου Εισοδημάτων	% του Συνόλου Αριθμού Φορολογουμένων	% του Συνόλου Εισοδημάτων
(0 - 12.000]	65.0%	35.8%	78.1%	25.8%	98.2%	58.3%
(12.000 - 42.000]	34.1%	58.3%	17.5%	39.4%	1.6%	21.3%
> 42.000	0.8%	5.9%	4.4%	34.8%	0.2%	20.4
Σύνολο	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**

Ποιοι φοροδιαφεύγουν;

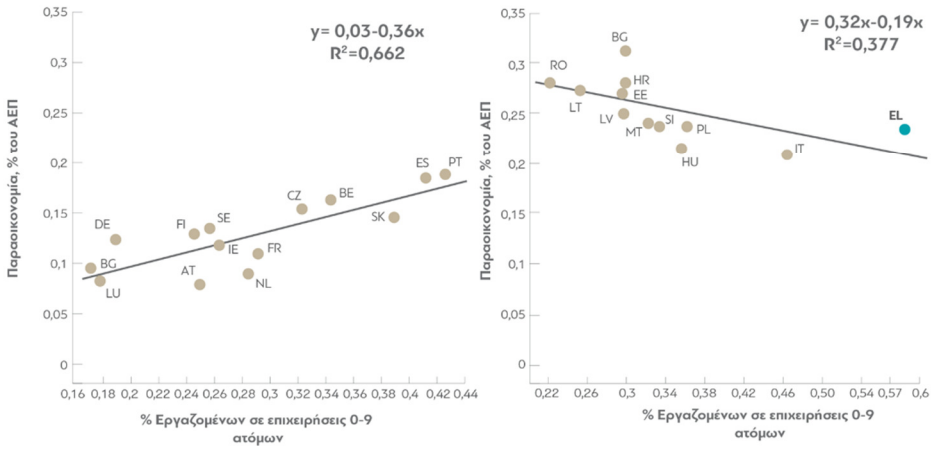
Υπάρχει μια αλήθεια που, λίγο-πολύ, ισχύει σε όλες τις χώρες του κόσμου: **Οι αυτοαπασχολούμενοι και οι πολύ μικρές επιχειρήσεις φοροδιαφεύγουν**. Από τις Ηνωμένες Πολιτείες μέχρι τη Γερμανία, και από την Ιταλία μέχρι τη Βουλγαρία, παντού οι πολύ μικρές επιχειρήσεις και πολλοί ελεύθεροι επαγγελματίες κατά κανόνα δηλώνουν στις Αρχές μικρότερο ποσοστό του εισοδήματός τους από ό,τι οι μισθωτοί ή οι μεγάλες επιχειρήσεις, επειδή η πιθανότητα εντοπισμού τους είναι παντού πολύ χαμηλή, και το κίνητρο να κόψουν αποδείξεις και να δηλώσουν τα εισοδήματά τους μικρότερο. Παρ' όλη τη φορολογική κουλτούρα, παρ' όλο το ύψος των προστίμων, μια πολύ μικρή επιχείρηση

στη Γερμανία μπορεί κάλλιστα να μην κόβει αποδείξεις για μέρος των πωλήσεών της χωρίς να εντοπιστεί, και χωρίς συνέπειες (Γεωργακόπουλος, 2016).

Αυτό το φαινόμενο έχει μικρότερες συνέπειες στα φορολογικά έσοδα των περισσότερων ανεπτυγμένων χωρών για έναν απλό λόγο: Επειδή οι πολύ μικρές επιχειρήσεις σε αυτές τις οικονομίες **είναι λίγες**, και οι αυτοαπασχολούμενοι **μικρό ποσοστό** του εργατικού δυναμικού. Αυτό είναι ένα πολύ σημαντικό χαρακτηριστικό όσον αφορά το πρόβλημα της φορολογίας στην Ελλάδα. Στην Ελλάδα **το ποσοστό της αυτοαπασχόλησης είναι διπλάσιο από τον αντίστοιχο Ευρωπαϊκό μέσο όρο** (34%). Σύμφωνα με μελέτες, το ποσοστό των μη-δηλωθέντων εισοδημάτων των αυτοαπασχολούμενων κυμαίνεται στο 57-58,6%, ενώ για τους μισθωτούς το αντίστοιχο ποσοστό είναι 0,5-1%. Οι απασχολούμενοι σε πολύ μικρές επιχειρήσεις (0-9 ατόμων) στην Ελλάδα είναι **διπλάσιοι** από ό,τι ισχύει στην Ε.Ε. -ένα ιλιγγιώδες **59%**. Το δε ποσοστό των εργαζομένων στις μεγάλες επιχειρήσεις (που απασχολούν παραπάνω από 250 υπαλλήλους) είναι **μόλις 13%** για την Ελλάδα, εν αντιθέσει με το 33% της Ε.Ε. Το πρόβλημα εδώ είναι ότι οι μικρές επιχειρήσεις μπορούν πιο εύκολα να απασχολούν αδήλωτους εργαζόμενους, αποφεύγοντας την καταβολή φορολογικών και ασφαλιστικών εισφορών, ενώ κόβουν σπανιότερα αποδείξεις και αποδίδουν λιγότερο ΦΠΑ (Γεωργακόπουλος, 2016).

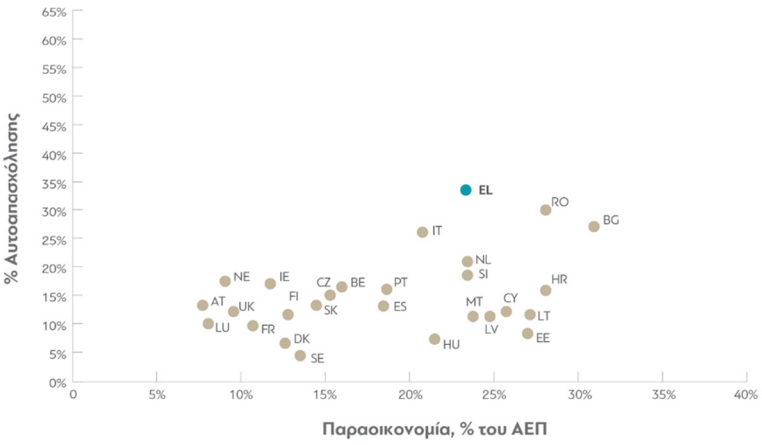
Σχέση Μεταξύ Παραοικονομίας, Απασχόλησης σε Πολύ Μικρές Επιχειρήσεις (0-9 Ατόμων) και Αυτοαπασχόλησης, 2014

Σχέση μεταξύ παραοικονομίας και απασχόλησης σε πολύ μικρές επιχειρήσεις (0-9 ατόμων)



Πηγή: Eurostat, Schneider (2015)

Παραοικονομία και αυτοαπασχόληση



Πηγή: Eurostat, Schneider (2015)

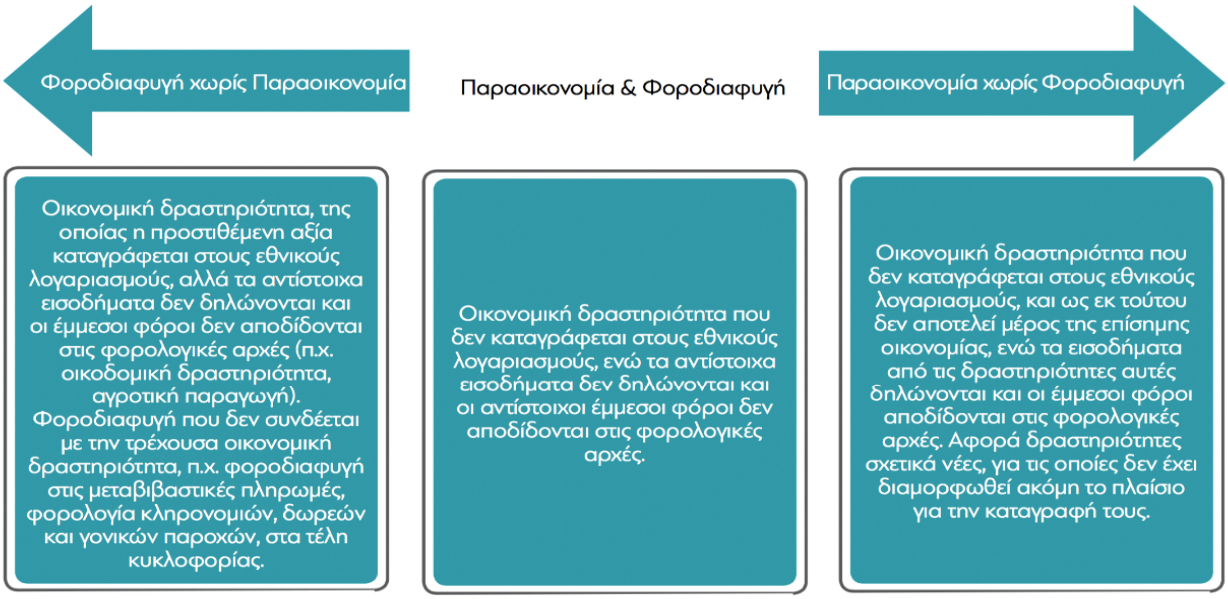
Πόσο φοροδιαφεύγουν οι πλούσιοι και οι μεγάλες επιχειρήσεις;

Κατά κανόνα, όπως είδαμε παραπάνω, οι πολίτες που έχουν υψηλά εισοδήματα πληρώνουν και την πλειοψηφία των φόρων στη χώρα. Ταυτόχρονα, όμως, πολίτες με πολύ υψηλά εισοδήματα -ένα πολύ *πολύ* μικρό υποσύνολο των 400.000 που δηλώνουν εισόδημα άνω των 42.000 ευρώ το χρόνο), έχουν στη διάθεσή τους μια σειρά από εργαλεία **φοροαποφυγής**, όπως την ίδρυση offshore εταιρειών, shell corporations, trusts και άλλων νομικών οντοτήτων. Σύμφωνα με μελέτες, το 8% της περιουσίας φορολογούμενων παγκοσμίως βρίσκεται σε φορολογικούς παραδείσους. Στην Ελλάδα, τα εργαλεία που χρησιμοποιούνται συχνότερα για το σκοπό αυτό σχετίζεται με τη μεταβίβαση ακινήτων σε

εξωχώριες εταιρείες (ένα φαινόμενο που μερικώς μπορεί να αντιμετωπιστεί με την επιβολή ενός ειδικού φόρου που τίθεται σε τέτοια ακίνητα) και αλλάζοντας φορολογική κατοικία, ενίοτε και με τεχνητά μέσα (Γεωργακόπουλος, 2016).

Η παραοικονομία

Η παραοικονομία λογίζεται ως όλες οι αδήλωτες οικονομικές συναλλαγές. Ως έννοια δεν είναι ίδια με τη φοροδιαφυγή, παρά σχετίζεται με ποικίλες αδήλωτες, "κρυφές" μυστικές δραστηριότητες που κυμαίνονται από το λαθρεμπόριο μέχρι τα ιδιαίτερα μαθήματα και ένα εστιατόριο που δεν παραδίδει στον πελάτη τα αντίστοιχα αποδεικτικά της λήψης της υπηρεσίας του (Γεωργακόπουλος, 2016).



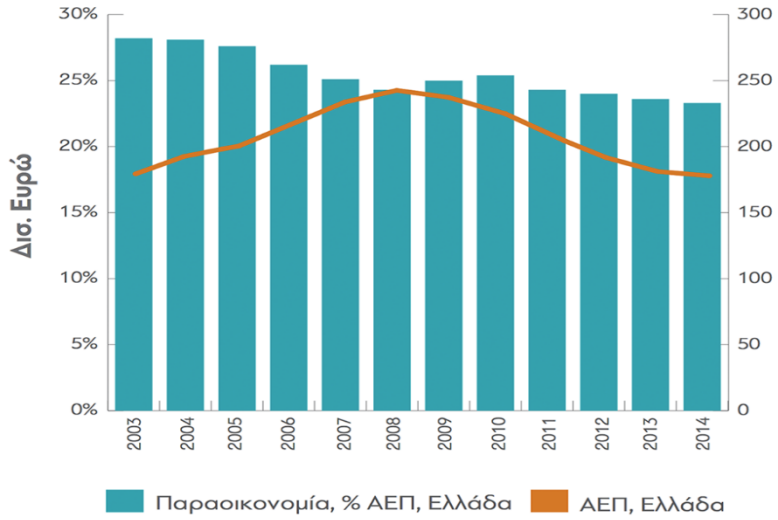
Πηγή: Προσαρμοσμένο από Βασαρδάνη Μ. (Ιούνιος 2011), *Φοροδιαφυγή στην Ελλάδα: Μια Γενική Επισκόπηση*, Οικονομικό Δελτίο Τεύχος 35, Τράπεζα της Ελλάδος. Βλ. επίσης και Νάστας Ε. (2007), *Το θεωρητικό πλαίσιο της διάκρισης ανάμεσα στη Φοροδιαφυγή και στην παραοικονομία*, e-Journal of Science & Technology (e-JST), Issue 4, σελ. 76, 86.

Παράγοντες που έχουν συμβάλλει στην παραοικονομία είναι:

1) Η αδήλωτη εργασία **25%** των εργαζομένων δεν είχε δηλωθεί. Τα χρόνια της κρίσης υπήρξε αύξηση δραματική και το 2013 είχε φτάσει στο **40,5%**.

Παραοικονομία ως Ποσοστό του ΑΕΠ και Οικονομική Δραστηριότητα (Ελλάδα & ΕΕ)

Γράφημα 20α: Παραοικονομία, % ΑΕΠ, Ελλάδα



Τι φταίει για τη φοροδιαφυγή;

Οι παράμετροι που είναι καθοριστικοί για το ύψος της φοροδιαφυγής είναι τρεις:

1. Το μέγεθος των φορολογικών συντελεστών
2. Η πιθανότητα να εντοπιστεί και να τιμωρηθεί
3. Το ύψος των προστίμων που επιβάλλονται

Το αν ένας πολίτης ή μια επιχείρηση μπορεί να φοροδιαφύγει ασκείται επιρροή από αυτούς τους τρεις παράγοντες. Αν οι φορολογικοί συντελεστές είναι χαμηλοί, το κίνητρο για φοροδιαφυγή είναι μικρότερο. Αν οι φοροεισπρακτικοί μηχανισμοί του κράτους είναι αναποτελεσματικοί στη λειτουργία τους, ή αν οι κυρώσεις στην περίπτωση σύλληψης είναι ελάχιστες, το κίνητρο φοροδιαφυγής είναι αυξανόμενο για κάποιον. Αυτό δεν ισχύει μόνο στην περίπτωση της Ελλάδας, παρά είναι αδιαμφισβήτητο γεγονός ότι η φοροδιαφυγή αποτελεί καθολικό φαινόμενο. Σημαντικό είναι επίσης πως και οι παράμετροι είναι παρόμοιες παντού.

Αν πρέπει εξειδικευτεί περισσότερο στην Ελλάδα, οι αιτίες φοροδιαφυγής είναι κυρίως οκτώ:

1. Η πολυνομία και το γεγονός ότι το φορολογικό σύστημα είναι περίπλοκο
2. Η ανασφάλεια δικαίου φορολογούμενων και υπαλλήλων της φορολογικής διοίκησης.

3. Η διαρκής άνοδος στους φόρους.
4. Η ανύπαρκτη πολιτική βούληση προκειμένου να αντιμετωπιστεί το φαινόμενο.
5. Τεχνολογική ανεπάρκεια
6. Γραφειοκρατία
7. Διαρθρωτικές στρεβλώσεις της ελληνικής οικονομίας
8. Φορολογική κουλτούρα

	Γερμανία	Φινλανδία	Πορτογαλία	Ρουμανία	Πολωνία	Ελλάδα		Πηγή:
Αυτοαπασχολούμενοι (% του συνόλου)	10,3%	12,1%	16,1%	30,1%	21,2%	33,8%		2013 AMECO
Εργαζόμενοι σε μικρές επιχειρήσεις (0-9 εργαζομένων) ως % του συνόλου	19,0%	24,5%	42,3%	22,5%	36,4%	58,6%		2012 Eurostat
Υστέρηση είσπραξης ΦΠΑ (VAT Gap)	10,6%	2,9%	8,7%	42,9%	25,3%	33,4%		2012 Eurostat
Ανώτερος συντελεστής ΦΠΑ	19,0%	24,0%	23,0%	24,0%	23,0%	23,0%		2015 European Commission
Τελικός φορολογικός συντελεστής στην κατανάλωση	19,8%	26,4%	18,1%	20,9%	19,3%	16,2%		2012 Eurostat
Τελικός φορολογικός συντελεστής στην εργασία	37,8%	40,1%	25,4%	30,4%	33,9%	38,0%		2012 Eurostat
Συνολικά φορολογικά έσοδα (% ΑΕΠ)	39,1%	44,1%	32,4%	28,3%	32,5%	33,7%		2012 Eurostat
Ηλεκτρονικές συναλλαγές κατά κεφαλήν	242,8	450,8	176,0	19,0	86,1	18,1		2013 ECB
ΑΕΠ κατά κεφαλήν (ευρώ)	32.600	35.500	15.600	6.600	9.900	17.400		2012 Eurostat
Παραοικονομία ως ποσοστό του ΑΕΠ	12,2%	12,9%	18,7%	28,1%	23,5%	23,3%		2014 Schneider
Αδήλωτη εργασία (ως ποσοστό συνόλου του εργατικού δυναμικού)	11,9%	11,2%	22,4%	11,8%	21,6%	46,7%		2011 World Bank
Αποτελεσματικότητα Δημόσιων Υπηρεσιών - Κυβέρνησης[1]	1,52	2,17	1,23	-0,07	0,71	0,45		2013 World Bank
Δείκτης Διαφθοράς[2]	1,78	2,19	0,91	-0,19	0,55	-0,11		2013 World Bank

Ποιες λύσεις υπάρχουν;

Θεωρείται πρόκληση η δυνατότητα να καταπολεμηθεί η φοροδιαφυγή για όλες τις χώρες ακόμα και αν είναι ανεπτυγμένες. Και στην περίπτωση της Ευρωπαϊκής Ένωσης και του ΟΟΣΑ αναπτύχθηκαν εργαλεία ώστε να καταπολεμηθεί η φοροδιαφυγή, ενώ η ιστορία που προυπήρχε αναφορικά με τις πολιτικές για την καταπολέμησή αυτού του προβλήματος από άλλες χώρες είναι σημαντικό να αναλυθεί κατόπιν μελέτης. Από τη στιγμή που χρησιμοποιείται πλαστικό χρήμα και επεκτείνονται οι ηλεκτρονικές συναλλαγές δοκιμάστηκαν πολλές χώρες σε γεωγραφικό μήκος και πλάτος από την Νότια Κορέα και την Αργεντινή έως και την Ολλανδία και τη Σουηδία. Είναι αξιοσημείωτη η εκσυγχρόνιση της φορολογικής διοίκησης στη Σιγκαπούρη, τη Βραζιλία αλλά και τη Βουλγαρία. Εκστρατείες ώστε να δημιουργηθεί φορολογική συνείδηση έχουν πραγματοποιηθεί επιτυχώς στην Ινδία, το Ισραήλ και το Μεξικό. Εξαιρετικά ήταν και τα αποτελέσματα αφότου συστάθηκε η Ανεξάρτητη Αρχή για την πάταξη της Διαφθοράς στο Χονγκ Κονγκ (Γεωργακόπουλος, 2016).

Δεν είναι όλα αυτά τα μέτρα εύκολα εφαρμόσιμα στη δική μας χώρα, αλλά πολλά από αυτά μπορούν να αποτελέσουν παραδείγματα προς μίμηση. Η έρευνα της διαΝΕΟσις καταλήγει σε μια σειρά από λύσεις που περιλαμβάνουν:

- **μείωση των συντελεστών φορολογίας** και των έκτακτων φόρων επί των ήδη φορολογηθέντων εισοδημάτων
- **εκτεταμένη χρήση πλαστικού χρήματος** και επέκταση της **ηλεκτρονικής τιμολόγησης**
- αποτελεσματική και εντατική **διενέργειας ελέγχων** και **αποτελεσματική περαίωσης** των φορολογικών υποθέσεων (μέσω διοικητικών και δικαστικών διαδικασιών)
- **βελτιστοποίηση της οργάνωσης** και **εκσυγχρονισμό** των φορολογικών αρχών
- δημιουργία **ηλεκτρονικής Φορολογικής Διοίκησης**
- **κατάρτιση** και **εκπαίδευση** των υπαλλήλων της Φορολογικής Διοίκησης, **αύξηση** των αποδοχών τους.
- καταπολέμηση φαινομένων **διαφθοράς**, εφαρμογή αντικινήτρων.
- **Αυστηρότερα πρόστιμα όταν προκύπτουν π**εριπτώσεις φοροδιαφυγής
- Σύσταση **φορολογικού συστήματος που είναι απλό και χαρακτηρίζεται από σταθερότητα**
- **Αλλαγή στη διάρθρωση** της ελληνικής οικονομίας που είναι σταδιακή
- πρόκληση **φορολογικής συνείδησης** και ώθηση υιοθέτησης **φορολογικής παιδείας**

Όπως μπορεί να γίνει κατανοητό από τα παραπάνω, υιοθετώντας τις προαναφερθείσες λύσεις και επιλύοντας το πρόβλημα συνιστά μια πολιτική απόφαση. Η φοροδιαφυγή στην Ελλάδα είναι ένα δύσκολο, δομικό πρόβλημα της ελληνικής οικονομίας, έχει να κάνει με τον τρόπο που αυτή είναι διαρθρωμένη, με τον πολύ μεγάλο αριθμό των αυτοαπασχολούμενων, με το πολύ μικρό μέσο μέγεθος των επιχειρήσεων. Οι πολιτικές ηγεσίες στο παρελθόν έχουν διστάσει να αντιμετωπίσουν αποτελεσματικά το πρόβλημα για πολιτικούς λόγους, διαιωνίζοντας την κουλτούρα ανομίας και, δικαιολογημένα, και την έλλειψη εμπιστοσύνης των πολιτών απέναντι στο κράτος. Και, βεβαίως, δεν έχουν κατορθώσει να αλλάξουν το αδιέξοδο παραγωγικό μοντέλο της χώρας. Ωστόσο, στην κατάσταση που βρίσκεται η ελληνική οικονομία σήμερα, η επίλυσή του προβλήματος είναι επιβεβλημένη και ίσως για πρώτη φορά και εφικτή. Κάποιες πρώτες κινήσεις για τον εκσυγχρονισμό της φορολογικής διοίκησης έχουν γίνει. Ίσως να υπάρχει περιθώριο να γίνουν περισσότερα. Οπωσδήποτε υπάρχει η ανάγκη (Γεωργακόπουλος, 2016).

1.2.3 Η ΜΟΛΥΝΣΗ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ

Μια επιχείρηση μπορεί να βλάψει το περιβάλλον είτε με την ταφή των αποβλήτων στο θαλάσσιο χώρο είτε με την υψηλή εκπομπή διοξειδίου του άνθρακα είτε με μόλυνση των υδάτων και με καταστροφή των χερσαίων δασικών ζωνών. Δηλαδή εν τέλει με την δραστηριοποίηση της. (Τσουραμάνης ,1996)

Από την δεκαετία του 1970 η Ευρωπαϊκή Ένωση έχει εγκρίνει περισσότερες από 200 νομοθετικές ρυθμίσεις για την προστασία του περιβάλλοντος. Στόχος όλων αυτών η αποτελεσματική εφαρμογή της νομοθεσίας. Παρόλα αυτά η μη τήρηση της νομοθεσίας έχει πολλές επιπτώσεις τόσο να υπονομεύσει θεμελιώδης περιβαλλοντικούς στόχους ,να βλάψει την δημοσιά υγειά , να προκαλέσει την οικονομική αβεβαιότητα του επιχειρηματικού κόσμου η ακόμα να βλάψει την δημοσιά υγειά. (europarl.europa.eu , 2014)

Σε αντίθετη περίπτωση η ορθή τήρηση της νομοθεσίας μπορεί να επιφέρει θετικά αποτελέσματα όπως οικονομικά οφέλη από το ίδιο το κράτος. Ενδεικτικά αν εφαρμόζονταν πλήρως η νομοθεσία για την διαχείριση των αποβλήτων θα μπορούσε να αποφέρει 400.000 νέες θέσεις εργασίας και να μειωθούν οι ετήσιες καθαρές δαπάνες κατά 72 εκατομμύρια ευρώ. (europarl.europa.eu , 2014)

Ένας τρόπος για την αξιοποίηση της προστασίας του περιβάλλοντος είναι η αγορά. Οι διάφοροι φόροι και επιδοτήσεις μπορούν να χρησιμοποιηθούν ενθαρρυντικά να παρακινηθούν οι επιχειρήσεις αλλά και οι καταναλωτές ώστε να επιλέγουν πιο οικολογικές μεθόδους παραγωγής και οι δε καταναλωτές να επιλέγουν τα πιο φιλικά προς το περιβάλλον προϊόντα. Εννοείται πως αυτές οι παραπάνω πολίτικες πρέπει να βασίζονται σε στοιχεία που επιτρέπουν την κατανόηση των αιτίων και των επιπτώσεών των περιβαλλοντικών μεταβολών έτσι ώστε να λαμβάνονται τα απαραίτητα μέτρα και η απαραίτητή κατάρτιση για να λειτουργήσει η κάθε στρατηγική. Η Ευρωπαϊκή ένωση μέσω διαφόρων προγραμμάτων ενισχύει όλη αυτή την προσπάθεια μεταβολής των επιχειρήσεων αλλά και των καταναλωτών στην αλλαγή αυτών των πολιτικών περί του περιβάλλοντος . (europarl.europa.eu , 2014)

Τέλος η ελληνική νομοθεσία περί της προστασίας του περιβάλλοντος ορίζει τα εξής:

Στην Ελληνική νομοθεσία υπάρχουν πριν από δεκαετίες προβλέψεις για την αντιμετώπιση ποινικών καταστάσεων κατά του περιβάλλοντος τόσο σε ποινικές όσο και σε διοικητικές κυρώσεις. Συγκεκριμένα σύμφωνα με το Άρθρο 24 παρ. 1 του Συντάγματος το 1975 κατοχυρώθηκε συνταγματικά η προστασία του περιβάλλοντος εν εποχή ΕΟΚ . Ενώ με τον ν. 743/77 όπως κωδικοποιήθηκε με το Π.Δ 55/1998 θεσπίστηκαν προβλέψεις για την προστασία του θαλάσσιου περιβάλλοντος και την συνέχεια με το ν. 3010/2002 προβλέπεται ρητά η ποινική τιμωρία για όποιον :

Α) προκαλεί ρύπανση ή υποβαθμίζει το περιβάλλον με πράξη ή παράλειψη που παραβαίνει στις διατάξεις του νόμου ή των διαταγμάτων που αναφέρονται ή υπουργικών αποφάσεων

Β) Ασκεί δραστηριότητα ή επιχείρηση χωρίς την απαιτούμενη σύμφωνα με τι ισχύουσες διατάξεις άδεια ή έγκριση ή υπερβαίνει τα όρια τις διατάξεις στην κοινοτική νομοθεσία.

Πράσινη ανάπτυξη και οικονομία. Πηγή: European commission.

1.2.4 Η ΕΞΑΠΑΤΗΣΗ ΤΩΝ ΚΑΤΑΝΑΛΩΤΩΝ

Αρκετές επιχειρήσεις όπως έχουμε αναφέρει για τον σκοπό μεγιστοποίησης των κερδών δηλαδή αύξηση πωλήσεων και παροχή περισσοτέρων υπηρεσιών στους

καταναλωτές διακινούν πολλές φορές προϊόντα που μπορεί να κριθούν επιβλαβή για το ευρύ καταναλωτικό κοινό σε συνδυασμό με αθέμιτες πρακτικές Συγκεκριμένα μπορεί :

α) να διακινούνται επικίνδυνα φάρμακα ή επιβλαβή τρόφιμα

β) διαφημίσεις που μπορεί να περιέχουν ψευδή χαρακτηριστικά των προϊόντων για την προσέλκυση καταναλωτικού κοινού και

γ) την κυκλοφορία ανασφαλών προϊόντων χωρίς την έγκριση ευρωπαϊκών προδιαγραφών (CE) ή αν αφορά τρόφιμα άδεια έγκρισης από τον ΕΦΕΤ ή αν πρόκειται για φάρμακα έγκριση από τον ΕΟΦ. (Τσουραμάνης , 1996)

Άλλωστε για αυτό δημιουργήθηκαν οι σχετικές πιστοποιήσεις ποιοτικού ελέγχου για κάθε μια ξεχωριστή κατηγορία αγαθών.

Αρχικά ο ΕΦΕΤ ο ενιαίος φορέας ελέγχου τρόφιμου δημιουργήθηκε στις 28-9-1999 Τελεί υπό την εποπτεία του Υπουργείου Αγροτικής ανάπτυξης και τροφίμων.

Οι Βασικές αρμοδιότητες είναι :

Α) η διεξαγωγή επιθεωρήσεων σε επιχειρήσεις τροφίμων ,ελέγχονται οι κανόνες ορθής βιομηχανικής πρακτικής και βιομηχανικής υγιεινής

Β) Ο απρόσκοπτος και συστηματικός έλεγχος των τροφίμων κατά την διακίνηση, εμπορία και διάθεση τους

Γ) η επικοινωνία με τον καταναλωτή με σκοπό την πληροφόρηση και εκπαίδευση του σε θέματα ασφάλειας των τροφίμων που καταναλώνει και η προστασία του έναντι από δόλιες πράξεις των επιχειρήσεων.

Δ) η αντιμετώπιση των διαφόρων διατροφικών κρίσεων στις επιχειρήσεις.

(Ε.Φ.Ε.Τ , 2021)

Στην συνέχεια ο ΕΟΦ (εθνικός οργανισμός φαρμάκων) ιδρύθηκε το 1983 και είναι Νομικό πρόσωπο δημοσίου δικαίου υπό την εποπτεία του Υπουργείου Υγείας.

Οι βασικές αρμοδιότητες είναι οι εξής :

α) αξιολόγηση και έγκριση ασφαλών και αποτελεσματικών προϊόντων.

Β) παρακολούθηση μετ. εγκριτικών προϊόντων για την ασφάλεια και την αποτελεσματικότητα στην χώρα

Γ) έλεγχος παραγωγής, κλινικών μελετών και αποτελεσματικότητας κανόνες ορθής παραγωγής των διαφόρων σκευασμάτων

Δ)ενημέρωση των επιστημόνων για τα νέα προϊόντα με σκοπό την ορθή χρήση και διάθεσης προς τους καταναλωτές.

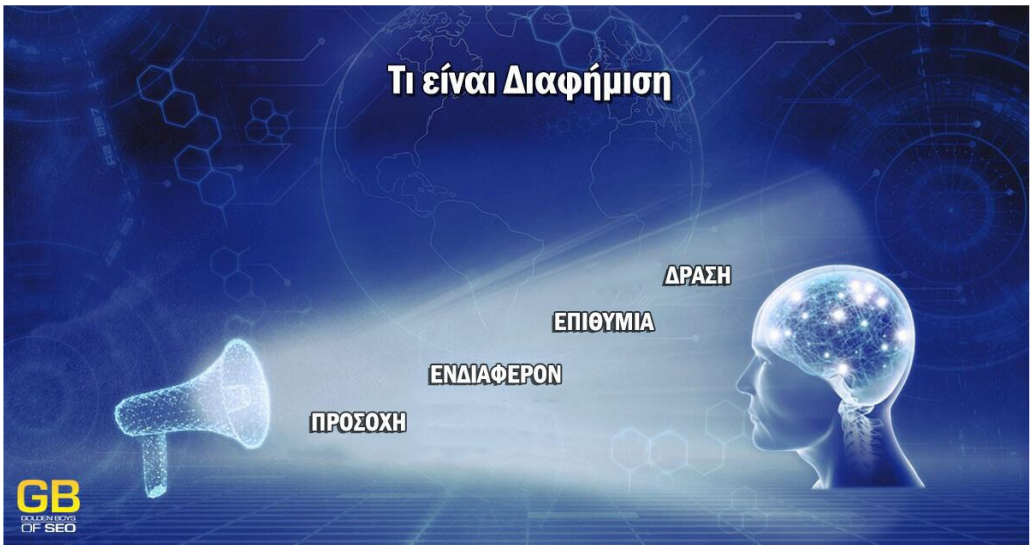
(Ε.Ο.Φ ,2021)

Τέλος η έγκριση CE (certification Europe) με το σήμα αυτό σε ένα προϊόν ο κατασκευαστής δηλώνει ότι το προϊόν αυτόν συμμορφώνεται με τις βασικές διατάξεις των ισχυουσών οδηγιών της Ευρωπαϊκής Ένωσης.

(Europa.eu, 2021)

Πάντως τα θέματα της παραπλανητικής και των αθέμιτων διαφημίσεων που χρησιμοποιούν σχεδόν όλες οι επιχειρήσεις στην επικράτεια καθώς και στο εξωτερικό , εδώ στην Ελλάδα ρυθμίζονται νομοθετικά από τις διατάξεις του ν. 2251 της 15/16-11-1994 περί προστασίας των καταναλωτών (ΦΕΚ Α 191) Περαιτέρω, όπως ορίζει η διάταξη, διαφήμιση λογίζεται ως η κάθε ανακοίνωση που γίνεται στα πλαίσια εμπορικής, βιομηχανικής, βιοτεχνικής ή επαγγελματικής δραστηριότητας με στόχο την προώθηση να διατεθούν αγαθά ή υπηρεσίες. Ως παραπλανητική διαφήμιση θεωρείται κάθε διαφημιστικό περιεχόμενο που προκαλεί ή πρόκειται να προκαλέσει παραπλάνηση ως προς τα άτομα που απευθύνεται. Η δε ταύτη παραπλάνηση μπορεί να ασκήσει επιρροή στην οικονομική συμπεριφορά των ατόμων αυτών (lawspot , 2021)

Τέλος Αθέμιτη σύμφωνα με την παράγραφο 5 του ιδίου Νόμου θεωρείται κάθε διαφήμιση που προσβάλει τα χρηστά ήθη.



Τι είναι διαφήμιση . Πηγή: golden boys of SEO

1.3 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΗΣ ΟΙΚΟΝΟΜΙΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Σε όλα όσα έχουν αναφερθεί στις παραπάνω παραγράφους στόχος αυτής την παραγράφου είναι να αναφέρουμε μερικούς τρόπους αντιμετώπισης αυτών των παραβάσεων .Με αλλά λογία να θέσουμε την ηθική των επιχειρήσεων σε μια άλλη κατεύθυνση έτσι ώστε να είναι επικερδείς αλλά να προτάσσουν το κοινωνικό σύνολο προπάντων . Σε αυτό θα βοηθούσε και ο κοινωνικός έλεγχος που μπορεί να ασκηθεί από όλους εμάς τους καταναλωτές.(Τσουραμάνης , 1996)

Όπως αναφέραμε οι καταναλωτές είναι εκείνοι που μπορούν να σταθούν απέναντι των επιχειρήσεων με την ανάλογη συμπεριφορά τους αλλά θα πρέπει η δράση αυτή να είναι συλλογική όχι να επικρατεί στην μειοψηφία αυτών . Οι δε αποφάσεις που θα παίρνουν συλλογικά οι καταναλωτές θα πρέπει να εμπίπτουν σε ρεαλιστικά γεγονότα δηλαδή να μην βλάπτουν τις επιχειρήσεις αλλά να εμποδίζουν τις δραστηριότητες δηλαδή την κριτική στάση απέναντι στην δραστηριοποίηση των επιχειρήσεων που αφορούν την εξαπάτηση την προστασία του περιβάλλοντος την φοροδιαφυγή και αλλά πολλά. (Τσουραμάνης ,1996)

Επομένως και το ίδιο το κράτος με την επιβολή σκληρότερων και αυστηρότερων νόμων να τιμωρεί πιο σκληρά σε σχέση με τη υπάρχουσα νομοθεσία και πρέπει εξυπακούεται να εφαρμόζονται όλοι οι νόμοι σε όλη τους την έκταση και να μην υπάρχουν περιθώρια καταπάτησης.

1.4 ΤΟ ΟΙΚΟΝΟΜΙΚΟ ΕΓΚΛΗΜΑ

Το οικονομικό έγκλημα, αναφέρεται σε παράνομες πράξεις που διαπράττονται από ένα άτομο ή μια ομάδα ατόμων για την απόκτηση οικονομικού ή επαγγελματικού πλεονεκτήματος. Το κύριο κίνητρο σε τέτοια εγκλήματα είναι το οικονομικό όφελος.

Η απάτη, τα οικονομικά και οικονομικά εγκλήματα αποτελούν μία από τις προτεραιότητες της ΕΕ για την καταπολέμηση του σοβαρού και οργανωμένου εγκλήματος στο πλαίσιο του EMPACT 2022 - 2025. Οι τομείς οικονομικού εγκλήματος που παρουσιάζουν ιδιαίτερο ενδιαφέρον για τις κοινές ομάδες έρευνας της Europol περιλαμβάνουν:

- Απάτη MTIC (Missing Trader Intra Community Fraud), η οποία περιλαμβάνει την εγκληματική εκμετάλλευση των κανόνων του φόρου προστιθέμενης αξίας (ΦΠΑ) στην ΕΕ, με αποτέλεσμα την απώλεια εσόδων να φτάνει τα δισεκατομμύρια ευρώ για τα κράτη μέλη.

- Απάτη στους ειδικούς φόρους κατανάλωσης, η οποία αναφέρεται στο λαθρεμπόριο αγαθών με υψηλή φορολογία, όπως ο καπνός, το αλκοόλ και τα καύσιμα·
- Ξέπλυμα βρώμικου χρήματος, η διαδικασία να φαίνονται νόμιμα τα προϊόντα εγκληματικής δραστηριότητας.

(Επίσημος Ιστότοπος της Ε. Ε., 2022)

Ο χαμηλός κίνδυνος και τα υψηλά κέρδη που συνδέονται με το οικονομικό έγκλημα το καθιστούν μια πολύ ελκυστική δραστηριότητα για ομάδες οργανωμένου εγκλήματος. Η πιθανότητα εντοπισμού και δίωξης της απάτης είναι μικρή λόγω της πολυπλοκότητας των απαιτούμενων ερευνών. Αυτό ισχύει ιδιαίτερα για περιπτώσεις απάτης που μπορούν να αποκαλυφθούν μόνο μέσω διεθνούς συνεργασίας, και για αδικήματα στο Διαδίκτυο για τα οποία πρέπει να καθοριστεί δικαιοδοσία.

Οι οργανωμένες εγκληματικές ομάδες που δρουν σε διεθνές επίπεδο επωφελούνται από τις διαφορές στην εθνική νομοθεσία. Ατομικές και οργανωτικές ευπάθειες, όπως η έλλειψη ευαισθητοποίησης από την πλευρά των θυμάτων και η αντίληψη χαμηλού κινδύνου από τις ομάδες-στόχους είναι παράγοντες που ευνοούν τους περισσότερους τύπους απάτης.

Υπάρχει αυξημένη επίγνωση ότι ορισμένες πράξεις στον χρηματοπιστωτικό τομέα που κάποτε θεωρούνταν απλώς κακή επιχειρηματική πρακτική μπορεί στην πραγματικότητα να ήταν εγκληματικές. Οι εκτεταμένες αλόγιστες επενδύσεις, η παραπλανητική περιγραφή των οικονομικών καταστάσεων και η συνωμοσία για χειραγώγηση των διατραπεζικών επιτοκίων εμπίπτουν στον ορισμό του σοβαρού και οργανωμένου εγκλήματος.

Οι τεράστιες απώλειες που συνδέονται με την οικονομική απάτη υψηλού επιπέδου υπονομεύουν τα συστήματα κοινωνικής ασφάλισης και αποσταθεροποιούν τα οικονομικά συστήματα, υποδηλώνοντας έτσι ξεκάθαρα αποτυχία της αυτορρύθμισης. Η αξιολόγηση απειλών για το σοβαρό και οργανωμένο έγκλημα του 2017 (SOCTA) επισημαίνει μια σειρά από τομείς απάτης που απασχολούν ιδιαίτερα την Europol και τις αρχές επιβολής του νόμου στα κράτη μέλη. Αυτές οι περιοχές εγκληματικότητας, οι οποίες περιγράφονται λεπτομερέστερα παρακάτω, είναι:

- επενδυτική απάτη
- απάτη μαζικού μάρκετινγκ
- απάτη με εντολή πληρωμής
- ασφαλιστική απάτη

- απάτη οφέλους
- Απάτη για τις επιδοτήσεις της ΕΕ
- νοθεύσεις προμηθειών
- απάτη δανείων και στεγαστικών δανείων

(Επίσημος Ιστότοπος της Ε. Ε., 2022)

Η επενδυτική απάτη βασίζεται σε τεχνικές κοινωνικής μηχανικής – τη χρήση εξαπάτησης για τη χειραγώγηση ατόμων ώστε να αποκαλύψουν εμπιστευτικές ή προσωπικές πληροφορίες που ενδέχεται να χρησιμοποιηθούν για δόλιους σκοπούς – καθιστώντας ιδιαίτερα δύσκολη την αντιμετώπισή της. Αυτός ο τύπος απάτης μπορεί να είναι ιδιαίτερα επικερδής, καθώς μια έρευνα αποκαλύπτει ότι μια ομάδα οργανωμένου εγκλήματος απέφερε εκτιμώμενα κέρδη έως και 3 δισεκατομμύρια ευρώ από τη δραστηριότητα. Τα πιο κοινά συστήματα επενδυτικής απάτης στην ΕΕ είναι:

- Σχέδια λεβητοστασίου, όπου οι απατεώνες καλούν τα θύματά τους και τα πιέζουν να επενδύσουν σε ανύπαρκτες ή πολύ χαμηλής αξίας μετοχές. Οι εγκληματίες συχνά χρησιμοποιούν πλαστά έγγραφα και πιστοποιητικά για να παρουσιάσουν την εταιρεία και τις μετοχές τους ως νόμιμες.

- Σχέδια Ponzi, όπου οι απατεώνες προσελκύουν μια ομάδα αρχικών επενδυτών με υποσχέσεις πολύ υψηλών αποδόσεων σε πολύ σύντομο χρονικό διάστημα. Για να προσελκύσει περισσότερα θύματα, ο απατεώνας θα αρχίσει να αποπληρώνει τους αρχικούς επενδυτές χρησιμοποιώντας κεφάλαια που συγκεντρώθηκαν από πρόσθετους επενδυτές. Τελικά, οι επενδυτές μένουν με άδεια χέρια, όταν ο απατεώνας εξαφανίζεται με τα κεφάλαια, τα οποία έχουν ξεπλυθεί μέσω πολλών τραπεζικών λογαριασμών που διατηρούνται από διάφορες εταιρείες-προπέτασμα σε διαφορετικές δικαιοδοσίες.

- Συστήματα πυραμίδας, τα οποία είναι παρόμοια με τα σχήματα Ponzi. Ωστόσο, οι αρχικοί επενδυτές συμμετέχουν ενεργά και καλούνται να προσλάβουν νέους επενδυτές για να αποκομίσουν κέρδη.

- Στην απάτη μαζικού μάρκετινγκ, οι εγκληματίες χρησιμοποιούν μια ποικιλία μέσων επικοινωνίας, όπως τηλεφωνήματα, διαδίκτυο, μέσα κοινωνικής δικτύωσης, μαζική αλληλογραφία, τηλεόραση ή ραδιόφωνο, για να

επικοινωνήσουν με θύματα και να ζητήσουν χρήματα ή άλλα αντικείμενα αξίας σε μία ή περισσότερες δικαιοδοσίες. Για παράδειγμα, μεταξύ Μαΐου 2014 και Μαΐου 2015, μια ομάδα οργανωμένου εγκλήματος με έδρα το Ηνωμένο Βασίλειο απάτησε πάνω από 690.000 ευρώ από συνταξιούχους σε ολόκληρη τη χώρα. Παρουσιαζόμενοι ως αστυνομικοί, οι εγκληματίες επικοινώνησαν τηλεφωνικά με τα θύματα για να τα προειδοποιήσουν για τον κίνδυνο απάτης στην τράπεζά τους. Τα θύματα ενθαρρύνθηκαν να μεταφέρουν τις αποταμιεύσεις τους σε λογαριασμούς φύλαξης που ελέγχονται από τους απατεώνες.

- Η απάτη με διαταγές πληρωμής όπου οι εγκληματίες χρησιμοποιούν δόλιες εντολές μεταφοράς για να εξαπατήσουν οργανισμούς του ιδιωτικού και του δημόσιου τομέα. Συνήθως, οι επηρεαζόμενοι οργανισμοί δραστηριοποιούνται διεθνώς. Αυτός ο ολοένα και πιο κοινός τύπος απάτης αναφέρεται επίσης ως απάτη CEO, απάτη μέσω τραπεζικού εμβάσματος ή συμβιβασμός επιχειρηματικού email. Οι εγκληματίες βασίζονται σε τεχνικές κοινωνικής μηχανικής και κακόβουλο λογισμικό για να πραγματοποιήσουν αυτού του είδους την απάτη. Συνήθως, τα κλεμμένα κεφάλαια μεταφέρονται μέσω σειρών λογαριασμών σε διάφορα κράτη μέλη πριν φτάσουν σε λογαριασμούς προορισμού εκτός ΕΕ.

- Η ασφαλιστική απάτη περιγράφει την εξαπάτηση ιδιωτικών και δημόσιων ασφαλιστικών φορέων. Ομάδες οργανωμένου εγκλήματος εμπλέκονται όλο και περισσότερο σε προγράμματα απάτης που στοχεύουν τα συστήματα υγειονομικής περίθαλψης.

- Η απάτη σχετικά με τις παροχές περιλαμβάνει τη στόχευση συστημάτων κοινωνικών και εργασιακών παροχών και συνδέεται στενά με την εμπορία ανθρώπων και τη λαθρεμπόριο μεταναστών.

- Η απάτη για τις επιδοτήσεις της ΕΕ που συντελείται όταν οι εγκληματίες υποβάλλουν δόλιες αιτήσεις για επιχορηγήσεις ή διαγωνισμούς της ΕΕ. Συνήθως, αυτές οι εφαρμογές βασίζονται σε ψευδείς δηλώσεις, αναφορές προόδου και τιμολόγια.

- Η νοθεία των προμηθειών πραγματοποιείται όταν εγκληματικές ομάδες χρησιμοποιούν δωροδοκίες για να αντλήσουν πληροφορίες ή να επηρεάσουν άμεσα την αξιολόγηση των προσφορών προκειμένου να κερδίσουν διαγωνισμούς δημόσιας υπηρεσίας σε ανταγωνισμό με νόμιμες επιχειρήσεις. Αυτός ο τύπος χειραγώγησης είναι ιδιαίτερα αξιοσημείωτος στους τομείς της

ενέργειας, των κατασκευών, της τεχνολογίας των πληροφοριών και της διαχείρισης απορριμμάτων.

- Η απάτη δανείων και ενυπόθηκων δανείων περιλαμβάνει απατεώνες που χρησιμοποιούν πλαστά έγγραφα για να λάβουν τραπεζικά δάνεια, τα οποία δεν επιστρέφονται ποτέ.

(Επίσημος Ιστότοπος της Ε. Ε., 2022)

Επιπρόσθετα, η παραχάραξη χρημάτων παραμένει ένα σοβαρό πρόβλημα για τις προηγμένες οικονομίες, ενώ τα ηλεκτρονικά μέσα πληρωμής προσφέρουν στους εγκληματίες νέες ευκαιρίες να διαπράξουν απάτη.

Η ανάπτυξη της διαδικτυακής τραπεζικής και των ηλεκτρονικών μέσων πληρωμής ήταν ένα δίκοπο μαχαίρι για τους καταναλωτές και τις επιχειρήσεις. Ενώ έχει μειώσει την εξάρτηση από τα φυσικά μετρητά, έχει επίσης προσφέρει στους εγκληματίες νέες ευκαιρίες να διαπράξουν απάτη.

Η απάτη, τα οικονομικά και οικονομικά εγκλήματα αποτελούν μία από τις προτεραιότητες της ΕΕ για την καταπολέμηση του σοβαρού και οργανωμένου εγκλήματος στο πλαίσιο του EMPACT 2022 - 2025.

Ενώ η πλαστογραφία νομισμάτων αναμένεται να μειωθεί με την πάροδο του χρόνου καθώς τα μετρητά γίνονται λιγότερο σημαντικά στην ψηφιακή εποχή, τα τραπεζογραμμάτια δεν θα αντικατασταθούν εξ ολοκλήρου από ηλεκτρονικά μέσα πληρωμής.

Ως αποτέλεσμα, οι εγκληματίες θα συνεχίσουν να πλαστογραφούν χαρτονομίσματα. Οι πρώτες ύλες που χρησιμοποιούνται για την παραχάραξη νομισμάτων θα γίνουν ακόμη πιο ευρέως διαθέσιμες, ιδιαίτερα στο darknet, το κρυφό Διαδίκτυο που υπάρχει κάτω από τον «επιφανειακό ιστό».

Ως το παγκόσμιο σημείο επαφής για την καταπολέμηση της παραχάραξης του ευρώ, η Europol εμπλέκεται σε όλες τις σημαντικές έρευνες πλαστογραφίας νομισμάτων στην ΕΕ. Ο οργανισμός συντονίζει κοινές ομάδες έρευνας και παρέχει οικονομική και ιατροδικαστική υποστήριξη, καθώς και επιτόπια βοήθεια, σε εταίρους επιβολής του νόμου στην ΕΕ.

Η καταπολέμηση της απάτης πληρωμών —ιδίως εκείνη που αφορά πιστωτικές και χρεωστικές κάρτες— είναι μία από τις τρεις εντολές του Ευρωπαϊκού Κέντρου για το Έγκλημα στον κυβερνοχώρο (EC3) της Europol. Μέσω της κοινής ομάδας δράσης για το έγκλημα στον κυβερνοχώρο (J-CAT), έχει υποστηρίξει πολλές υψηλού προφίλ επιχειρήσεις και έρευνες για το έγκλημα στον κυβερνοχώρο, όπως το Operation Imperium, το οποίο

στόχευε ένα δίκτυο οργανωμένου εγκλήματος που δραστηριοποιείται στην απάτη πληρωμών.

Στην Αξιολόγηση απειλών για το οργανωμένο έγκλημα στο Διαδίκτυο του 2016 (IOCTA), η Europol συνέστησε οι αρχές επιβολής του νόμου της ΕΕ να επικεντρωθούν στους ακόλουθους επιχειρησιακούς τομείς:

- Κακόβουλο λογισμικό ATM και συσκευές skimming
- Απάτη στο ηλεκτρονικό εμπόριο με έμφαση στους τομείς των μεταφορών (αεροπορικές εταιρείες), του λιανικού εμπορίου και των καταλυμάτων.
- Η απόκτηση και διαπραγμάτευση παραβιασμένων οικονομικών δεδομένων

Η Europol έχει επίσης εντείνει τη δράση κατά των υποθέσεων απάτης CEO στην Ευρώπη. Σε αυτές τις περιπτώσεις, οι απατεώνες που παρουσιάζονται ως ο Διευθύνων Σύμβουλος ή ως μέλος της ανώτερης διευθυντικής ομάδας μιας εταιρείας ξεγελούν έναν υπάλληλο της εταιρείας για να τους συνδέσουν κεφάλαια.

(Επίσημος Ιστότοπος της Ε.Ε., 2022)

ΚΕΦΑΛΑΙΟ 2 – ΨΗΦΙΑΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

2.1 ΕΝΝΟΙΑ ΨΗΦΙΑΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Με την εκτεταμένη χρήση των ηλεκτρονικών συσκευών (υπολογιστές , κινητά κτλ.) αλλά και με τη αθέμιτη χρήση των παραπάνω συσκευών αρκετά χρόνια τώρα έχει εμφανιστεί το φαινόμενο της ψηφιακής παραβατικότητας. Γι αυτό θα μπορούσαμε να αναφέρουμε τον εξής ορισμό. *« Κατά τον Mc Ewen ψηφιακή παραβατικότητα θεωρείται κάθε παράνομη πράξη για την τέλεση της οποίας είναι απαραίτητη η γνώση των τεχνολογικών συστημάτων»(Mc Ewen ,1989 ,Τσουραμανης 1996)*

Επιπλέον ως 'ηλεκτρονικό έγκλημα όπως αλλιώς αναφέρεται, μπορούμε να «*θεωρήσουμε τις αξιόποινες εγκληματικές πράξεις που τελούνται με την χρήση ηλεκτρονικών υπολογιστών και άλλων ψηφιακών μέσων και διώκονται με συγκεκριμένες ποινές από την ελληνική νομοθεσία*». Τα εγκλήματα αυτά μπορούν να χωριστούν ανάλογα με τον τρόπο τέλεσης σε εγκλήματα τελούμενα με χρήση ηλεκτρονικών υπολογιστών, και σε κυβερνοεγκλήματα που γίνονται μέσω του διαδικτύου. *(Ελληνική Αστυνομία , 2021)*

2.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΨΗΦΙΑΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Υπάρχουν πολλά χαρακτηριστικά γνωρίσματα για να συμπεριλάβουμε στην ψηφιακή παραβατικότητα. Αρχικά , το διαδικτυακό έγκλημα που είναι ευρέος διαδεδομένο στις σύγχρονες κοινωνίες μπορεί να συμβεί σε ελάχιστα δευτερόλεπτα. Η ταχύτητα που μπορεί να συμβεί είναι κυρίως η βασική αιτία που το θύμα δεν μπορεί να αντιληφθεί αυτό που του/της έχει συμβεί. Ο δράστης συνδέεται στο διαδίκτυο χρησιμοποιώντας ηλεκτρονικό υπολογιστή και εισβάλει σε διάφορα άλλα υπολογιστικά συστήματα άλλων χρηστών που μπορεί είτε να είναι ιδιωτικά υπολογιστικά συστήματα ή εταιρικά υπολογιστικά συστήματα οπουδήποτε σε όλον τον κόσμο με κύριο σκοπό την υποκλοπή δεδομένων. Επομένως είναι εύκολα κατανοητό για την ευκολία που μπορεί να τελεστεί από όλον τον κόσμο και κυρίως απρόσωπα. (Τσουραμάνης , 1996)

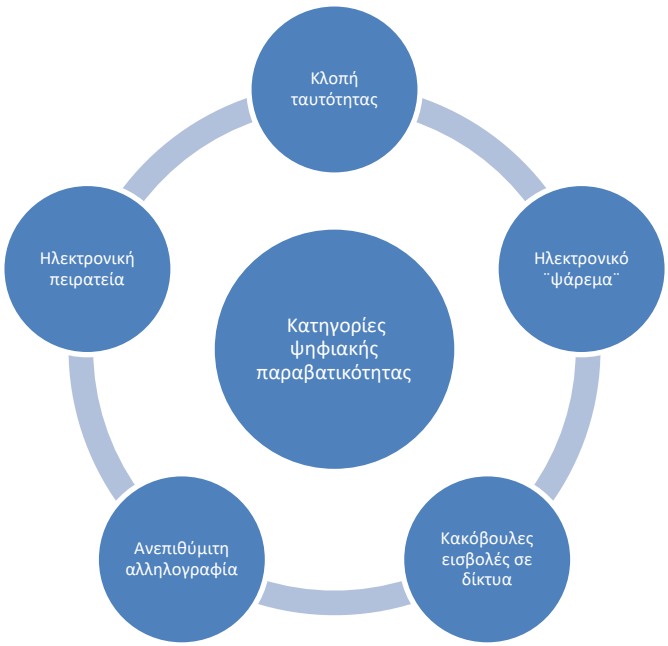
Στην συνέχεια , η ψηφιακή παράβαση δεν περιορίζεται μόνο στην υποκλοπή δεδομένων ,άλλα μπορεί και στην καταστροφή διαφόρων μερών ενός υπολογιστικού συστήματος όπως σε σκληρό δίσκο , μνήμες κτλ. Βέβαια αυτά θεωρούνται δευτερεύουσες συνέπειες ενός κύριου χτυπήματος. Επιπλέον, η εισβολή σε ένα υπολογιστικό σύστημα γίνεται ακόμα ευκολότερη με χρήση εφαρμογών ελευθέρου λογισμικού χαρακτήρα . Έπειτα , ως προς την διερεύνηση της ψηφιακής παραβατικότητας θα πρέπει ο ενδιαφερόμενος να έχει γνώσεις σε θέματα διαδικτύου – δικτύου , πληροφορικής καθώς και έχει ειδίκευση σε θέματα νομικά περί δίωξης και να έχει συνεργασία με τις αστυνομικές και δικαστικές αρχές.

Φυσικά σε τέτοιου είδους παραβάσεις προτείνεται και η συνεργασία με δυο ή περισσότερα κράτη για την διαλεύκανση της παράβασης.

Στατιστικά , τα νούμερα των περιστατικών τόσο στον διεθνή όσο και σε εγχώριο επίπεδο δεν είναι επαρκή καθώς ακόμα και αν αντιληφθεί ο χρήστης ότι βρίσκεται σε ηλεκτρονική απάτη συνήθως δεν θα το καταγγείλει στις αρχές λόγω φόβου και στην περίπτωση των επιχειρήσεων για να μην υποθάλψουν το κύρος που έχουν σε δημόσιο επίπεδο. Άρα δεν έχουμε πραγματικό δείγμα στατιστικών για να βγάλουμε ασφαλή συμπεράσματα κατά ποσό επηρεάζει παγκοσμίως η ψηφιακή παραβατικότητα.

2.3 ΚΑΤΗΓΟΡΙΕΣ ΨΗΦΙΑΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Γενικότερα το έγκλημα στον κόσμο του διαδικτύου κυμαίνεται σε ένα φάσμα δραστηριοτήτων. Στην πρώτη περίπτωση βρίσκονται διάφορες παραβάσεις της προσωπικής ή εταιρικής ζωής. Μέσα σε αυτό συμπεριλαμβάνεται και το πολύ συχνό έγκλημα της κλοπής κάποιας ταυτότητας. Στα μέσα του φάσματος βρίσκονται εγκλήματα που σχετίζονται με απάτη σε συναλλαγές ,ηλεκτρονική πειρατεία και γενικότερα με εγκλήματα που σχετίζονται κυρίως με την ανωνυμία στο διαδίκτυο .Στο άλλο άκρο του φάσματος είναι εκείνα τα εγκλήματα που συμπεριλαμβάνουν απόπειρες παραβίασης των κανόνων του διαδικτύου όπως τα ανεπιθύμητη αλληλογραφία και η κυβερνοτρομοκρατία ακόμα και η κακόβουλη εισβολή στα δίκτυα δηλαδή η χρήση του διαδικτύου που προξενεύει δημόσιες αναταραχές και σε ακραίες περιπτώσεις μέχρι και θάνατο παράδειγμα κυβερνοτρομοκρατίας μπορεί να θεωρηθεί και η επίθεση στους δίδυμους πύργους της 11ης Σεπτεμβρίου 2001 (Dennis ,2021).



Κατηγορίες ψηφιακής παραβατικότητας

2.3.1 ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Το συγκεκριμένο είδος εγκλήματος επηρεάζει τόσο στον εικονικό όσο και στο πραγματικό κόσμο αλλά οι επιπτώσεις σε κάθε μια περίπτωση είναι διαφορετικές για παράδειγμα στην Ελλάδα για να εισπραχτούν οι φόροι υπάρχει ο αριθμός φορολογικού μητρώου. Επίσης με τον συγκεκριμένο αριθμό μπορεί να χρησιμοποιηθεί και για άλλες λειτουργιές του κράτους όπως υγεία ,πρόνοια. Άρα είναι εύκολα κατανοητό ότι από έναν απλό κωδικό αριθμό μπορούν οι εισβολείς να χρησιμοποιήσουν αυτό το στοιχειό για την κλοπή πολλών στοιχείων για την ιδιωτική αλλά και επαγγελματική ζωή ενός ατόμου και στην χειρότερη περίπτωση την αναδημιουργία της ταυτότητας του συγκεκριμένου ατόμου με ψευδείς πληροφορίες. Όσο αναφορά σε εταιρικό επίπεδο οι εγκληματίες μπορούν να κλέψουν αρχεία εταιρικών λογαριασμών μιας εταιρίας για να τα χρησιμοποιήσουν με ποικίλους τρόπους. Ένα σημαντικό παράδειγμα είναι η δημιουργία εικονικών τραπεζικών λογαριασμών με αποτέλεσμα οι εταιρίες που έχουν πέσει θύματα να υποστούν μεγάλες χρηματικές απώλειες. (Dennis , 2021)

2.3.2 ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ (PHISHING)

Σε αυτή την περίπτωση ο δράστης μέσω διαφόρων μηνυμάτων που στέλνει στα θύματα θέλει να αποσπάσει προσωπικά οικονομικά στοιχειά όπως κωδικούς τραπέζης. Συνήθως με ψευδή στοιχειά αυτό-αποκαλούνται ως η ιδία η τράπεζα και με αυτό τον τρόπο μέσω μιας ψεύδους πλατφόρμας το θύμα να δίνει τα προσωπικά του στοιχειά τόσο εύκολα στον δράστη. Στην συνεχεία οι απατεώνες χρησιμοποιούν αυτά τα δεδομένα εις βάρος του ιδίου του χρηστή για δημιουργία αξιόποινων πράξεων. Είναι ο πλέον διαδεδομένος σύγχρονος τρόπος κλοπής στοιχείων λόγω της τεράστιας ψηφιακής ανάπτυξης τα τελευταία 5 χρόνια. Άλλωστε γιαυτο και οι τράπεζες θωρακίζουν τα sites τους προκειμένου οι πελάτες τους να απολαμβάνουν μια ασφαλή εμπειρία πλοήγησης στις τραπεζικές συναλλαγές τους,(Τσουραμάνης ,2005).

2.3.3 ΚΑΚΟΒΟΥΛΕΣ ΕΙΣΒΟΛΕΣ ΣΕ ΔΙΚΤΥΑ

Οι κακόβουλες εισβολές σε δίκτυα ή αλλιώς και hacking είναι η μη εξουσιοδοτημένη και χωρίς έγκριση εισβολή σε έναν ηλεκτρονικό υπολογιστή όπου κύριος σκοπός είναι κυρίως η επιβεβαίωση των ικανοτήτων των εισβολέων να προσβάλουν ένα υπολογιστικό σύστημα. Παρόλα αυτά, ορισμένες φορές μπορεί να χρησιμοποιηθεί και για αποκόμιση οικονομικών οφελών ή ακόμα και για καταστροφή ενός υπολογιστικού συστήματος. Αυτό συμβαίνει γιατί ο επιτιθέμενος εισβάλει στο υπολογιστικό σύστημα του θύματος εντοπίζει τα αδύνατα σημεία και έτσι με την βοήθεια αλγορίθμων μπορεί να διαπράξει την

συγκεκριμένη αξιόποινη πράξη. Επιπλέων αυτού του τύπου οι παραβάσεις χρησιμοποιούνται περισσότερο και για την απειλή ορισμένων πιθανών δημόσιων προσώπων προς ικανοποίηση ορισμένων κοινών συμφερόντων ιδίως σε μεγάλες ηπείρους όπως αυτή των Ηνωμένων πολιτειών της Αμερικής μέσω διαφόρων μυστικών υπηρεσιών πολύ δραστηριοποιούνται σε τέτοιου είδους επιθέσεις.

2.3.4 ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

Η ανεπιθύμητη αλληλογραφία ή διαφορετικά spamming ονομάζεται η μαζική αποστολή μηνυμάτων σε υπολογιστή τα οποία έχουν συνήθως εμπορικό στόχο και αποστέλλονται σε μεγάλη μερίδα ατόμων. Κύριος στόχος αυτών των μηνυμάτων είναι να εξαπατήσουν τους ανυποψίαστους χρήστες για να αντλήσουν με παράνομο τρόπο προσωπικά τους στοιχεία. Είναι ο πλέον πιο διαδεδομένος τρόπος δράσης παρατατικών συμμοριών τόσο στην Ελλάδα όσο και στο εξωτερικό εξαιτίας της μεγάλης ευκολίας που υπάρχει στην σύγχρονη εποχή λόγω της μεγάλης χρήσης πολλών σταθερών και φορητών συσκευών (κινητά τηλέφωνα ,tablets).

2.3.5 ΗΛΕΚΤΡΟΝΙΚΗ ΠΕΙΡΑΤΕΙΑ

Αρχικά, ηλεκτρονική πειρατεία λογίζεται η ηθελημένη καταπάτηση των πνευματικών δικαιωμάτων για παράνομη εμπορική χρήση. Για την δημιουργία ηλεκτρονικού εμπορίου χρειάζεται η κατασκευή ενός χώρου στο διαδίκτυο όπου θα δύναται η πρόσβαση διαφόρων πελατών και η δημιουργία συναλλαγών. Για να εισέλθουν σε αυτούς τους χώρους το λεγόμενο όνομα πεδίου ή όνομα χώρου όπως ονομάζεται επιτρέποντας στον χρήστη του διαδικτύου τη διασύνδεση με τον κάτοχο της ηλεκτρονικής διεύθυνσης. Υπάρχουν τρεις περιπτώσεις πειρατείας. (IFPI 2012)

Η φυσική πειρατεία θεωρείται η αναπαραγωγή σε υλικούς φορείς ήχου ή εικόνας χωρίς την συγκατάθεση αυτού που διαθέτει τα δικαιώματα. Εννοείται πως αναφερόμαστε σε δραστηριότητες με εμπορικό σκοπό . (IFPI 2012)

Τα παραχαραγμένα αρχεία αποτελούν τα μη εξουσιοδοτούμενα αντίγραφα που μοιάζουν κατά μεγάλο βαθμό με τα γνήσια. Τα διάφορα σχέδια ή εικόνες αναπαράγονται συνοδευόμενα από τα επίσημα σήματα των αληθινών παραγωγών έτσι ώστε ο ανυποψίαστος αγοραστής να πιστεύει ότι έχει αγοράσει το αυθεντικό προϊόν. (IFPI 2012)

Η διαδικτυακή πειρατεία είναι το σύνολο μη εξουσιοδοτούμενων χρήσεων ψηφιακών αρχείων στο διαδίκτυο. Απώτερος σκοπός είναι η δημιουργία κέρδους από αυτές τις δραστηριότητες για τους παραβάτες. Οι πράξεις αυτές δημιουργούν ένα τεράστιο εμπορικό και οικονομικό πρόβλημα στους αυθεντικούς δημιουργούς και τέλος θίγει τα πνευματικά δικαιώματα του ιδίου του δημιουργού.(IFPI 2012)

Τα πνευματικά δικαιώματα αναφορικά, είναι οι κανόνες εκείνοι που ορίζει ο δημιουργός ενός καλλιτεχνικού ή ψηφιακού έργου στα οποία ορίζει με ποιον τρόπο θα χρησιμοποιηθούν ή θα φτάσουν στο κοινό(IFPI 2012).

2.3.6 ΕΓΚΛΗΜΑ ΥΨΗΛΗΣ ΤΕΧΝΟΛΟΓΙΑΣ (HIGH TECH CRIME)

Μια μορφή εγκλήματος στον κυβερνοχώρο, το έγκλημα υψηλής τεχνολογίας αναφέρεται σε εγκλήματα που χρησιμοποιούν ηλεκτρονική και ψηφιακά βασισμένη τεχνολογία για να επιτεθούν σε υπολογιστές ή σε δίκτυο υπολογιστών.

Τέτοια εγκλήματα περιλαμβάνουν την παραβίαση υπολογιστών ή οποιαδήποτε μη εξουσιοδοτημένη χρήση ή διανομή δεδομένων, επιθέσεις άρνησης υπηρεσίας και διανομή ιών υπολογιστών.

Οι εγκληματίες υψηλής τεχνολογίας χρησιμοποιούν μια σειρά εργαλείων κακόβουλου λογισμικού, που κυμαίνονται από τραπεζικά trojans μέχρι ransomware και phishing, για να οργανώσουν τις επιθέσεις τους. Κακόβουλο λογισμικό διεισδύει και αποκτά τον έλεγχο ενός συστήματος υπολογιστή ή μιας κινητής συσκευής για να κλέψει πολύτιμες πληροφορίες ή να καταστρέψει δεδομένα. Υπάρχουν πολλοί τύποι κακόβουλου λογισμικού και μπορούν να αλληλοσυμπληρώνονται κατά την εκτέλεση μιας επίθεσης.

Το Adware εμφανίζει διαφημιστικά banner ή αναδυόμενα παράθυρα που περιλαμβάνουν κώδικα για την παρακολούθηση της συμπεριφοράς του χρήστη στο διαδίκτυο.

Ένας trojan backdoor/απομακρυσμένης πρόσβασης (RAT) έχει πρόσβαση σε σύστημα υπολογιστή ή φορητή συσκευή εξ αποστάσεως. Μπορεί να εγκατασταθεί από ένα άλλο κομμάτι κακόβουλου λογισμικού. Παρέχει σχεδόν απόλυτο έλεγχο στον εισβολέα, ο οποίος μπορεί να εκτελέσει ένα ευρύ φάσμα ενεργειών, όπως:

- δράσεις παρακολούθησης
- εκτέλεση εντολών
- αποστολή αρχείων και εγγράφων πίσω στον εισβολέα
- πληκτρολόγηση καταγραφής
- λήψη στιγμιότυπων οθόνης

Ένα botnet (συντομογραφία για το δίκτυο ρομπότ) αποτελείται από υπολογιστές που επικοινωνούν μεταξύ τους μέσω του Διαδικτύου. Ένα κέντρο εντολών και ελέγχου τα χρησιμοποιεί για την αποστολή ανεπιθύμητων μηνυμάτων, την προσάρτηση κατανεμημένων επιθέσεων άρνησης υπηρεσίας (DDoS) και τη διάπραξη άλλων εγκλημάτων.

Ένα αρχείο infector μολύνει εκτελέσιμα αρχεία (όπως .exe) αντικαθιστώντας τα ή εισάγοντας μολυσμένο κώδικα που τα απενεργοποιεί.

Το Ransomware εμποδίζει τους χρήστες να έχουν πρόσβαση στις συσκευές τους και απαιτεί πληρωμή λύτρων μέσω ορισμένων τρόπων ηλεκτρονικής πληρωμής για να ανακτήσουν την πρόσβαση. Μια παραλλαγή, το αστυνομικό ransomware, χρησιμοποιεί σύμβολα επιβολής του νόμου για να δώσει εξουσία στο μήνυμα λύτρων.

Το Scareware είναι ψεύτικο λογισμικό προστασίας από ιούς που προσποιείται ότι σαρώνει και βρίσκει κακόβουλο λογισμικό/απειλές ασφαλείας στη συσκευή ενός χρήστη, ώστε να πληρώσει για να το αφαιρέσει.

Το λογισμικό κατασκοπείας εγκαθίσταται σε έναν υπολογιστή χωρίς να το γνωρίζει ο ιδιοκτήτης του για να παρακολουθεί τη δραστηριότητά του και να μεταδίδει τις πληροφορίες σε τρίτους.

Το rootkit είναι μια συλλογή προγραμμάτων που επιτρέπουν την πρόσβαση σε επίπεδο διαχειριστή σε έναν υπολογιστή ή ένα δίκτυο υπολογιστών, επιτρέποντας έτσι στον εισβολέα να αποκτήσει πρόσβαση root ή προνομιακή πρόσβαση στον υπολογιστή και πιθανώς σε άλλα μηχανήματα στο ίδιο δίκτυο.

Ένας trojan αποτελεί ή είναι ενσωματωμένο σε ένα νόμιμο πρόγραμμα, αλλά έχει σχεδιαστεί για κακόβουλους σκοπούς, όπως η κατασκοπεία, η κλοπή δεδομένων, η διαγραφή αρχείων, η επέκταση ενός botnet και η εκτέλεση επιθέσεων DDoS.

Ένας ιός τύπου worm αναπαράγεται μέσω ενός δικτύου υπολογιστών και εκτελεί κακόβουλες ενέργειες χωρίς καθοδήγηση.

Το ακμάζον επιχειρηματικό μοντέλο διαδικτυακού εγκλήματος ως υπηρεσία παρέχει συνεχώς στους εγκληματίες πρόσβαση σε μεγάλο αριθμό τεχνικών εγκλήματος στον κυβερνοχώρο.

(Επίσημος Ιστότοπος Ε. Ε, 2022)

2.3.7. ΤΟ ΨΗΦΙΑΚΟ ΕΓΚΛΗΜΑ ΤΗΝ ΠΕΡΙΟΔΟ ΤΗΣ ΠΑΝΔΗΜΙΑΣ

Σύμφωνα με την Interpol οι κυβερνοαπειλές εξελίσσονται διαρκώς προκειμένου να επωφεληθούν από τη συμπεριφορά και τις τάσεις στο διαδίκτυο. Το ξέσπασμα του COVID-19 δεν αποτελεί εξαίρεση.

Οι κυβερνοεγκληματίες επιτίθενται στα δίκτυα και τα συστήματα υπολογιστών ατόμων, επιχειρήσεων, ακόμη και παγκόσμιων οργανισμών, σε μια εποχή που η άμυνα στον κυβερνοχώρο ενδέχεται να μειωθεί λόγω της μετατόπισης της εστίασης στην κρίση υγείας.

Υπάρχει ένας σημαντικός αριθμός καταχωρημένων τομέων στο Διαδίκτυο που περιέχουν τους όρους: "coronavirus", "corona-virus", "covid19" και "covid-19".

Ενώ ορισμένοι είναι νόμιμοι ιστότοποι, οι εγκληματίες του κυβερνοχώρου δημιουργούν χιλιάδες νέους ιστότοπους κάθε μέρα για να πραγματοποιούν καμπάνιες ανεπιθύμητης αλληλογραφίας, ηλεκτρονικό ψάρεμα ή να διαδώσουν κακόβουλο λογισμικό.

Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται τις εκτεταμένες παγκόσμιες επικοινωνίες για τον κορονοϊό για να κρύψουν τις δραστηριότητές τους. Κακόβουλο λογισμικό, λογισμικό υποκλοπής spyware και Trojans έχουν βρεθεί ενσωματωμένα σε διαδραστικούς χάρτες και ιστότοπους για τον κορονοϊό. Τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου εξαπατούν επίσης τους χρήστες να κάνουν κλικ σε συνδέσμους που κατεβάζουν κακόβουλο λογισμικό στους υπολογιστές ή τις κινητές συσκευές τους.

Νοσοκομεία, ιατρικά κέντρα και δημόσια ιδρύματα γίνονται στόχος κυβερνοεγκληματιών για επιθέσεις ransomware – καθώς έχουν κατακλυστεί από την υγειονομική κρίση και δεν μπορούν να αντέξουν οικονομικά να αποκλειστούν από τα συστήματά τους, οι εγκληματίες πιστεύουν ότι είναι πιθανό να πληρώσουν τα λύτρα.

Το ransomware μπορεί να εισέλθει στα συστήματά του μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν μολυσμένους συνδέσμους ή συνημμένα, παραβιασμένα διαπιστευτήρια υπαλλήλων ή εκμεταλλευόμενά μια ευπάθεια στο σύστημα.

(Εεπίσημος Ιστότοπος Interpol, 2022)

2.4 ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΗΣ ΨΗΦΙΑΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

2.4.1 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΟΥ ΚΑΛΥΠΤΕΙ ΤΗΝ ΨΗΦΙΑΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

Αρχικά, στην ελληνική νομοθεσία δεν υπάρχει αποκλειστικός νόμος που να προστατεύει κατά απόλυτο βαθμό τα ηλεκτρονικά εγκλήματα. Ο νόμος 1805/88 αφορά τα εγκλήματα που διαπράττονται με την χρησιμοποίηση ηλεκτρονικού υπολογιστή. Υπάρχουν και σχετικές τροποποιήσεις στον ποινικό κώδικα (άρθρα 13γ 370β 370γ 386^{α})οι οποίες συνδέονται με την διάπραξη εγκλημάτων μέσω ψηφιακών συσκευών. Επίσης το άρθρο 370^{α} σχετίζεται στην παραβίαση του απορρήτου των τηλεπικοινωνιών και το άρθρο 348^{α} στην πορνογραφία ανηλίκων. Τα παραπάνω άρθρα στο ποινικό κώδικα δεν επαρκούν για την πάταξη της ηλεκτρονικής εγκληματικότητας η οποία με τις τεχνολογικές βελτιώσεις δημιουργούν νέες περιπτώσεις.

Όταν δημιουργήθηκε ο νόμος εννοείται ότι δεν ήταν τόσο διαδεδομένη η χρήση του διαδικτύου που πλέον είναι το κυρίαρχο εργαλείο για την ηλεκτρονική εγκληματικότητα. Βέβαια αυτό το νομικό κενό αντιμετωπίζεται με την υπάρχουσα νομοθεσία σαν ένα συμβατικό έγκλημα διότι θεωρείται από τον νομοθέτη ότι το διαδίκτυο είναι ένα μέσο για την διάπραξη κακόβουλων ενεργειών.(Φλώρου,2013)

Επίσης, υφίσταται η διάταξη για την ανεπιθύμητη αλληλογραφία (Π.Δ 131/2003) όπου αναφέρεται στην κακόβουλη τεχνική του spamming και στην ευθύνη των παροχών υπηρεσιών δικτύου για τις πράξεις των πελατών τους. Επιπλέον το παραπάνω προεδρικό διάταγμα δημιουργήθηκε με την εμφάνιση του ηλεκτρονικού εμπορίου. Εν ‘συνεχεία ο νόμος 2867/2000 για την οργάνωση και τη λειτουργία των τηλεπικοινωνιών, οι νόμοι 2774/1999 και 2472/1997 περί προσωπικών δεδομένων και ο νόμος 2225/1994 περί της προστασίας της ελευθερίας ανταπόκρισης και επικοινωνίας (σε αντικατάσταση με τον νόμο 3115/2003)με την ίδρυση της εθνικής επιτροπής απορρήτου και επικοινωνιών.(lawspot ,2021)

Σε ευρωπαϊκό επίπεδο η Ευρώπη προσέγγισε το θέμα του ηλεκτρονικού εγκλήματος στο συμβούλιο της Ευρώπης στο Στρασβούργο το 1976 που παρουσιάστηκαν για πρώτη φορά οι μορφές του ηλεκτρονικού εγκλήματος.

Το 1996 το συμβούλιο της Ευρώπης δημιούργησε τρεις συστάσεις οι οποίες εκείνη την εποχή δεν είχαν δεσμευτικό χαρακτήρα για τα κράτη-μέλη. Η πρώτη είναι η σύσταση No R (1989) 9 που σχετίζεται με το έγκλημα που γίνεται μέσω υπολογιστή, η δεύτερη σύσταση No R(1995) 13 για τα δικονομικά ζητήματα που σχετίζονται με τις πληροφορίες,

Η τελευταία και πιο πρόσφατη σύσταση No R(2001) 8 σχετίζεται με ρυθμιστικά στοιχεία στο θέμα του διαδικτύου.

2.4.2 ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΗΣ ΨΗΦΙΑΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Το απόρρητο έχει αναγνωριστεί ως σημαντικό πρόβλημα στη διαχείριση και η σημασία του θα συνεχιστεί να κλιμακώνεται καθώς η αξία των πληροφοριών συνεχίζει να αυξάνεται. Η κατανόηση και προστασία του προσωπικού απορρήτου σε πληροφοριακά συστήματα γίνεται ολοένα και πιο κρίσιμη με ευρεία χρήση δικτυωμένων συστημάτων και του Διαδικτύου. Αυτές οι τεχνολογίες παρέχουν ευκαιρίες συλλογής μεγάλων ποσών προσωπικών πληροφοριών σχετικά με διαδικτυακούς χρήστες, πιθανώς δηλώνοντας το προσωπικό απόρρητο αυτών των χρηστών. Οργανώσεις έχουν αναλάβει να εμφανίζουν τις πολιτικές απορρήτου του ιστότοπού τους στο διαδίκτυο. Αυτό είναι εν μέρει ένας τρόπος περιορισμού της πιθανής νομικής ευθύνης μέσω αποποιήσεις ευθυνών. Περίπου οι μισοί νέοι επισκέπτες σε ένα δεδομένο ιστότοπο ηλεκτρονικού εμπορίου λένε ότι διαβάζουν την πολιτική απορρήτου του οργανισμού. Οι επισκέπτες του ιστότοπου μπορούν να βγάλουν συμπεράσματα σχετικά με τον οργανισμό από την πολιτική απορρήτου του ιστότοπου. Κάποιοι παρατηρητές επέκριναν αυτές τις πολιτικές, καθώς έκριναν ότι είναι πολύ αδύναμες ή πολύ περίπλοκες. Οι ερευνητές έχουν σημειώσει ότι οι καταναλωτές εξετάζουν εάν μία δεδομένη οργάνωση είναι μια οργάνωση στην οποία θα ένιωθαν καλά ώστε να προβούν σε συναλλαγές μαζί τους ως μέρος των αποφάσεων συναλλαγών τους (Earp et al, 2005).

Επιπλέον, οι καταναλωτές κάνουν αυτήν την αξιολόγηση με βάση τα «σήματα» από τον οργανισμό (Earp et al, 2005). Για παράδειγμα, ο οργανισμός δημοσίευσε πολιτικές απορρήτου που μπορεί να θεωρηθούν ως ένα μήνυμα για την αξιόπιστη ύπαρξη ενός οργανισμού. Εάν οι πολιτικές απορρήτου δηλώνονται σαφώς και ρητά, τότε αντιλαμβάνεται ο επισκέπτης/καταναλωτής τον οργανισμό ως πιο αξιόπιστο. Αυτό, με τη σειρά του, βοηθά τον οργανισμό να προσελκύει νέους πελάτες και να διατηρεί τους υπάρχοντες. Βεβαίως, ισχύει και το αντίστροφο, έτσι ώστε ένας οργανισμός με περισσότερες ύποπτες πολιτικές μπορεί να έχουν πρόβλημα να εξασφαλίσουν νέους πελάτες ή να διατηρήσουν τους προηγούμενους. Οι προηγούμενοι πελάτες που έρχονται δύσπιστοι μπορεί να προκαλέσουν ζητήματα σε έναν ανταγωνιστή, να νιώθουν επιφυλακτικοί στην αποκάλυψη τυχόν πρόσθετων, μεταγενέστερων πληροφοριών· ή να αναρτήσουν για την επιχείρηση μια κακή από στόμα σε στόμα κριτική.

Πρακτικές, όπως οι δηλώσεις πολιτικής, που αντιμετωπίζουν την ανησυχία του πελάτη σχετικά με τις υβριστικές προσωπικές πληροφορίες έχουν ως αποτέλεσμα θετικές εμπειρίες με ένα οργανισμό και ως αποτέλεσμα να αυξηθεί η αντίληψη του πελάτη ότι ο

οργανισμός μπορεί να είναι αξιόπιστος (Earp et al, 2005). Έτσι, οι πολιτικές απορρήτου και οι δηλώσεις πολιτικής για τα συμφέροντα των πελατών μπορούν πιθανόν να επηρεάσουν τα αποτελέσματα ενός οργανισμού. Γιατί αυτά οι πολιτικές μπορεί να είναι τόσο σημαντικές, το απόρρητο, οι πληροφορίες, το μάρκετινγκ, και οι υπεύθυνοι δημοσίων σχέσεων επιφορτίζονται με την αύξηση πρόκληση εξισορρόπησης των συμφερόντων των πελατών με τους οργανωτικούς στόχους. Αυτοί οι διευθυντές δεν είναι οι μόνοι επαγγελματίες που επηρεάζονται από ζητήματα απορρήτου. Διευθυντές μηχανικής λογισμικού και διαχειριστές έργου πρέπει να βεβαιωθούν ότι η λειτουργικότητα του συστήματος ταιριάζει με τους ισχυρισμούς της δήλωσης απορρήτου. Για παράδειγμα, δύο πρόσφατες μελέτες βρήκαν αποκλίσεις μεταξύ των δηλώσεων απορρήτου και των πραγματικών πρακτικών απορρήτου σε οργανισμούς. Η ευθυγράμμιση των αξιώσεων πολιτικής και λειτουργικότητας είναι μία σύνθετη δραστηριότητα, φέρνοντας και τα δύο σε ευθυγράμμιση με τους χρήστες που είναι κάτι ακόμη πιο δύσκολο. Η λειτουργικότητα του συστήματος έχει άμεσο αποτέλεσμα για τις απαιτήσεις του συστήματος, ως εκ τούτου, την επίτευξη αυτού του είδους Η ευθυγράμμιση ξεκινά με την εξέταση στη φάση των απαιτήσεων της ανάπτυξης ιστοσελίδων. Αν η αναπτυξιακή προσπάθεια πρόκειται να είναι επιτυχημένη, στη συνέχεια χρήστες, αναλυτές, προγραμματιστές και διαχειριστές πρέπει να συνεργάζονται κατά τη φάση των απαιτήσεων λογισμικού. Αξίζει να τονιστεί συνεπώς πως όπως προαναφέρθηκε πραγματοποιούνται αρκετές παραβιάσεις στο διαδίκτυο και για αυτό είναι κρίσιμο να αντιμετωπιστούν. Διάφοροι τρόποι ως προς αυτό είναι η πιστοποίηση χρήστη, το λογισμικό ασφαλείας – λογισμικό antivirus, ο τοίχος προστασίας, η αποφυγή κοινοποίησης προσωπικών δεδομένων και στοιχείων (Earp et al, 2005).

ΠΙΣΤΟΠΟΙΗΣΗ ΧΡΗΣΤΗ

Η συνήθης ταυτοποίηση του χρήστη είναι η δημιουργία ενός ονόματος χρήστη και ενός κωδικού πρόσβασης προκειμένου να επιτρέπεται η προσβασιμότητα σε ευαίσθητα αρχεία του συστήματος από συγκεκριμένους εξουσιοδοτημένους χρήστες. Αυτή η διαδικασία μπορεί να χρησιμεύσει στην χρήση του διαδικτύου ή στην προσπέλαση διαφόρων ευαίσθητων προσωπικών στοιχείων σε έναν υπολογιστή. Θα πρέπει ο χρήστης του υπολογιστή να λάβει υπόψη την τακτική αλλαγή των στοιχείων πρόσβασης με διαφορετικές λέξεις ή σύμβολα προς αποτροπή σπασίματος των εκάστοτε στοιχείων πρόσβασης. (Φλώρου , 2013)

ΛΟΓΙΣΜΙΚΟ ΑΣΦΑΛΕΙΑΣ - ΛΟΓΙΣΜΙΚΟ ANTIVIRUS

Η μετάδοση των ιών είναι μια από τις ποιο συνηθισμένες μορφές ψηφιακής παραβατικότητας. Η ανάπτυξη πολλών νέων ιών θεωρείται πλέον μια πολύπλοκη απειλή για όλες τις ηλεκτρονικές συσκευές. Η χρήση λογισμικών ασφαλείας είναι η πιο αξιόπιστη

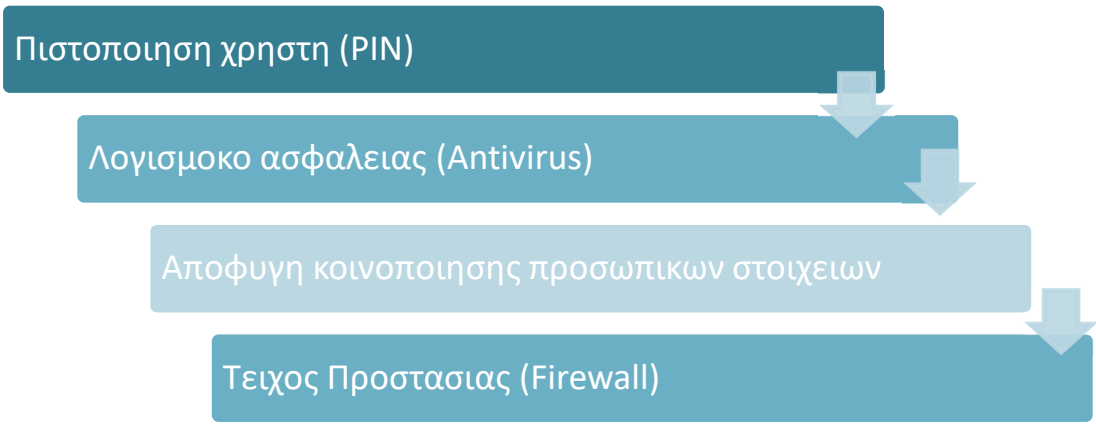
μέθοδος αποτροπής τους. Είναι απαραίτητο να βρίσκεται εγκατεστημένο σε όλες τις ηλεκτρονικές συσκευές προς αποφυγή ζημιών (Φλώρου , 2013)

ΤΟΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (FIREWALL)

Στους υπολογιστές το τοίχος προστασίας χρησιμοποιείται για την εποπτεία πακέτων δεδομένων ή προγραμμάτων οδήγησης που περνούν μέσω δικτύου από τον ένα υπολογιστή στον άλλον. Η βασική χρήση του τοίχους προστασίας είναι η εποπτεία ενός τοπικού δικτύου ανάμεσα στα δίκτυα των υπολογιστών. Συνηθίζεται η μεγαλύτερη κατόπτευση να δίδεται στα μη έμπιστα δίκτυα όπως είναι το διαδίκτυο. Ενώ το εταιρικό ή τοπικό δίκτυο μιας εταιρείας ή ενός σπιτιού αντίστοιχα διαθέτουν τον υψηλότερο βαθμό εμπιστευτικότητας .Εννοείται πως όπως και τα αντιβιοτικά προγράμματα έτσι και το τοίχος προστασίας βοηθάει στην πρόληψη των επιθέσεων σε ένα τοπικό δίκτυο και την αντιμετώπιση τους. (Φλώρου , 2013)

ΑΠΟΦΥΓΗ ΚΟΙΝΟΠΟΙΗΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Προς ατομικής προστασίας του ιδίου του χρήστη του διαδικτύου που επισκέπτεται καθημερινά πολλές ιστοσελίδες ένας ακόμα τρόπος προφύλαξης είναι η μη κοινοποίηση προσωπικών και ευάλωτων πληροφοριών του στο διαδίκτυο. Πιο συγκεκριμένα ο χρήστης θα πρέπει να ελέγχει στην ιστοσελίδα που πρόκειται να συμπληρώσει προσωπικά στοιχειά του τον βαθμό ασφαλείας της ιστοσελίδας αλλά και τους όρους προστασίας προσωπικών δεδομένων που πιθανόν συμπεριλαμβάνονται στην ιστοσελίδα. Επιπρόσθετα για τον ίδιο τον χρήστη κάλο θα ήταν όπου είναι δυνατό να αποφεύγει την προσθήκη ευάλωτων προσωπικών πληροφοριών του δηλαδή αριθμό τηλεφώνου , αριθμό φορολογικού μητρώου , διεύθυνση κατοικίας του ,αστυνομική ταυτότητα κ.α. καθώς ακόμα και η καλύτερη δομημένη ιστοσελίδα δεν μπορεί να μένει απροσπέλαστη από παράνομες εισβολές. Συνεπώς προσεκτικά, αποφεύγουμε την εισαγωγή ευάλωτων πληροφοριών στο διαδίκτυο.



Τρόποι αντιμετώπισης της ψηφιακής παραβατικότητας

Το ηλεκτρονικό έγκλημα δεν γνωρίζει σύνορα. Οι εγκληματίες του κυβερνοχώρου βρίσκουν συνεχώς νέους τρόπους για να επωφεληθούν από τα εγκλήματά τους σε βάρος των πολιτών, των επιχειρήσεων και των κυβερνήσεων, πέρα από τα εθνικά σύνορα και τις δικαιοδοσίες.

Έτσι, οι αστυνομικές δυνάμεις σε όλο τον κόσμο αντιμετωπίζουν παρόμοια εγκλήματα στον κυβερνοχώρο και παρόμοιους εγκληματικούς στόχους, και αυτό απαιτεί μια συντονισμένη, διεθνή προσέγγιση του προβλήματος.

Η κοινή ομάδα δράσης για το έγκλημα στον κυβερνοχώρο (J-CAT), η οποία ξεκίνησε τον Σεπτέμβριο του 2014. Βρίσκεται στο Ευρωπαϊκό Κέντρο για το έγκλημα στον κυβερνοχώρο (EC3) της Europol και βοηθά στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο εντός και εκτός της ΕΕ.

Ο στόχος του J-CAT είναι να καθοδηγεί από πληροφορίες, συντονισμένη δράση κατά των βασικών απειλών και στόχων του εγκλήματος στον κυβερνοχώρο, διευκολύνοντας τον κοινό εντοπισμό, τον καθορισμό προτεραιοτήτων, την προετοιμασία, την έναρξη και την εκτέλεση διασυνοριακών ερευνών και επιχειρήσεων από τους εταίρους του. Αντιμετωπίζει:

- εγκλήματα που εξαρτώνται από τον κυβερνοχώρο·
- διακρατική απάτη πληρωμών·
- διαδικτυακή σεξουαλική εκμετάλλευση παιδιών·

- διευκολύνσεις στον κυβερνοχώρο διασταυρούμενων εγκλημάτων (π.χ. αλεξίσφαιρη φιλοξενία, υπηρεσίες κατά των ιών, εγκληματική χρήση του σκοτεινού ιστού κ.λπ.).

  (Επίσημος Ιστότοπος της Ε.Ε., 2022)

Η ομάδα εργασίας είναι ανοιχτή σε περιστασιακές συνεισφορές, κατά περίπτωση, από μη συμμετέχουσες χώρες και μη εταίρους επιβολής του νόμου. Αυτό μπορεί επίσης να γίνει στο πλαίσιο ενός προγράμματος επισύναψης J-CAT, το οποίο προβλέπει μια προσωρινή κατάσχεση για συνεργασία σε μια υπόθεση εγκλήματος στον κυβερνοχώρο με συνδέσμους με τουλάχιστον δύο τρέχουσες χώρες μέλη του J-CAT. Σχετικά με το J-CAT ισχύουν τα ακόλουθα στοιχεία:

- Αποτελείται από μια μόνιμη επιχειρησιακή ομάδα αξιωματικών συνδέσμων στον κυβερνοχώρο από πολλά κράτη μέλη της ΕΕ και εταίρους συνεργασίας εκτός ΕΕ, οι οποίοι εδρεύουν στα κεντρικά γραφεία της Europol και συμπληρώνονται από το προσωπικό της EC3.

- Οι αξιωματικοί σύνδεσμοι στον κυβερνοχώρο προέρχονται από:10 κράτη μέλη της ΕΕ (Αυστρία, Βέλγιο, Γαλλία, Γερμανία, Ιταλία, Ολλανδία, Ρουμανία, Πολωνία, Σουηδία και Ισπανία, η οποία εκπροσωπείται από δύο υπηρεσίες: Policía Nacional και Guardia Civil)).

- 7 χώρες εταίροι εκτός ΕΕ (Αυστραλία, Καναδάς, Κολομβία, Νορβηγία, Ελβετία, Ηνωμένο Βασίλειο και Ηνωμένες Πολιτείες, οι οποίες εκπροσωπούνται από τρεις υπηρεσίες: το Ομοσπονδιακό Γραφείο Ερευνών, τη Μυστική Υπηρεσία και την Υπηρεσία Εσωτερικών Εσόδων).

- Αποτελεί το Ευρωπαϊκό Κέντρο για το έγκλημα στον κυβερνοχώρο (EC3) της Europol.

- Όλοι οι αξιωματικοί του εργάζονται από το ίδιο γραφείο για να διασφαλίσουν ότι μπορούν να επικοινωνούν εύκολα μεταξύ τους.

- Επιπλέον, ένας ειδικός Εθνικός Εμπειρογνώμονας αποσπασμένος από την Eurojust στην EC3 της Europol συνεργάζεται τακτικά με την EC3 και την J-CAT για να συζητήσει υποθέσεις και έργα αμοιβαίου ενδιαφέροντος.

- Το J-CAT επιλέγει και ιεραρχεί ποιες υποθέσεις θα ακολουθήσει βάσει, μεταξύ άλλων, προτάσεων από τους αξιωματικούς συνδέσμους της χώρας. Τα μέλη:

- επιλέγουν τις πιο σχετικές προτάσεις.
- μοιράζονται, συλλέγουν και εμπλουτίζουν δεδομένα για τις εν λόγω περιπτώσεις·
- αναπτύσσουν ένα σχέδιο δράσης, το οποίο καθοδηγείται από τη χώρα που υπέβαλε την επιλεγμένη πρόταση·
- περνούν όλα τα απαραίτητα βήματα για να διασφαλίσουν ότι η υπόθεση είναι έτοιμη να γίνει στόχος δράσης επιβολής του νόμου — μια διαδικασία που περιλαμβάνει διαβούλευση με τις δικαστικές αρχές, τον εντοπισμό των απαιτούμενων πόρων και την κατανομή των ευθυνών.

- Το J-CAT διοικείται από ένα συμβούλιο που αποτελείται από τουλάχιστον έναν ανώτερο εκπρόσωπο επιβολής του νόμου ανά συμμετέχουσα υπηρεσία. Το διοικητικό συμβούλιο διευθύνεται από μια χώρα-πρόεδρο και έναν αντιπρόεδρο-χώρα, που εκλέγονται απευθείας από το ίδιο το συμβούλιο. Το Συμβούλιο J-CAT, μαζί με το EC3, καθορίζει τη στρατηγική κατεύθυνση και αντιμετωπίζει τακτικά και επιχειρησιακά θέματα.

  (Επίσημος Ιστότοπος της Ε.Ε., 2022)

2.4.2.1 Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος: EC3

Η Europol ίδρυσε το Ευρωπαϊκό Κέντρο για το Έγκλημα στον κυβερνοχώρο (EC3) το 2013 για να ενισχύσει την απάντηση των αρχών επιβολής του νόμου στο έγκλημα στον κυβερνοχώρο στην ΕΕ και έτσι να βοηθήσει στην προστασία των ευρωπαίων πολιτών, επιχειρήσεων και κυβερνήσεων από το διαδικτυακό έγκλημα. Από την ίδρυσή του, το EC3 έχει συμβάλει σημαντικά στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο: έχει συμμετάσχει σε δεκάδες επιχειρήσεις υψηλού προφίλ και εκατοντάδες επιτόπιες αναπτύξεις επιχειρησιακής υποστήριξης με αποτέλεσμα εκατοντάδες συλλήψεις και έχει αναλύσει εκατοντάδες χιλιάδες αρχείων , η συντριπτική πλειοψηφία των οποίων έχει αποδειχθεί κακόβουλο. Αν και είναι δύσκολο να παρασχεθούν αξιόπιστες εκτιμήσεις, ορισμένες εκθέσεις του κλάδου υποδηλώνουν ότι το παγκόσμιο κόστος του εγκλήματος στον κυβερνοχώρο ανέρχεται σε εκατοντάδες δισεκατομμύρια ευρώ ετησίως.

Κάθε χρόνο, η EC3 δημοσιεύει την Εκτίμηση Απειλών για το Οργανωμένο Έγκλημα στο Διαδίκτυο (IOCTA), την κορυφαία στρατηγική της έκθεση σχετικά με τα βασικά ευρήματα και τις αναδυόμενες απειλές και εξελίξεις στο έγκλημα στον κυβερνοχώρο.

Η IOCTA καταδεικνύει πόσο ευρύ και ποικίλο είναι το έγκλημα στον κυβερνοχώρο και πώς το EC3 αποτελεί βασικό μέρος της αντίδρασης της Europol και της ΕΕ. Το EC3 υιοθετεί μια τριπλή προσέγγιση για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο: εγκληματολογία, στρατηγική και επιχειρήσεις.

Το Συμβούλιο Προγράμματος EC3 παρέχει στην EC3 οδηγίες σχετικά με το πώς να επιτύχει τους στόχους της και να εκπληρώσει τα επίσημα καθήκοντά της, βασιζόμενη σε συνεργασίες, κοινή ευθύνη και συνεργασία με όλα τα μέλη του διοικητικού συμβουλίου.

Το EC3 έχει δύο ομάδες εγκληματολογίας, την ψηφιακή εγκληματολογία και την εγκληματολογία εγγράφων, καθεμία από τις οποίες επικεντρώνεται στην επιχειρησιακή υποστήριξη και στην έρευνα και ανάπτυξη.

Υπάρχουν δύο ομάδες στρατηγικής, η πρόληψη και η διαχείριση των ενδιαφερομένων, η οποία δημιουργεί εταιρικές σχέσεις, διασφαλίζει την ανάπτυξη τυποποιημένης κατάρτισης και συντονίζει τα μέτρα πρόληψης και ευαισθητοποίησης και η ομάδα στρατηγικής και ανάπτυξης, η οποία είναι υπεύθυνη για: στρατηγική ανάλυση, τη διαμόρφωση πολιτικής και νομοθετικών μέτρων, τη διακυβέρνηση του Διαδικτύου.

Σε επίπεδο επιχειρήσεων, το EC3 εστιάζει στους ακόλουθους τύπους εγκλημάτων στον κυβερνοχώρο:

- Έγκλημα που εξαρτάται από τον κυβερνοχώρο.
- Διαδικτυακή σεξουαλική εκμετάλλευση παιδιών.
- Απάτη πληρωμών.

Αυτές οι δραστηριότητες υποστηρίζονται επίσης από την Ομάδα Πληροφοριών στον κυβερνοχώρο (CIT), οι αναλυτές της οποίας συλλέγουν και επεξεργάζονται πληροφορίες που σχετίζονται με το έγκλημα στον κυβερνοχώρο από δημόσιες, ιδιωτικές και ανοιχτές πηγές και εντοπίζουν αναδυόμενες απειλές και πρότυπα.

Στο πλευρό του EC3 συνεργάζεται η κοινή ομάδα δράσης για το έγκλημα στον κυβερνοχώρο (J-CAT), η οποία εργάζεται στις πιο σημαντικές υποθέσεις διεθνούς εγκλήματος στον κυβερνοχώρο που επηρεάζουν τα κράτη μέλη της ΕΕ και τους πολίτες τους.

Το EC3 βασίζεται στην υπάρχουσα ικανότητα επιβολής του νόμου της Ευρωπόλ — αλλά επεκτείνεται επίσης σημαντικά σε άλλες δυνατότητες, ιδίως προσφέροντας επιχειρησιακή και αναλυτική υποστήριξη στις έρευνες των κρατών μελών.

Για καθεμία από τις τρεις κατηγορίες εγκλήματος στον κυβερνοχώρο, EC3:

- χρησιμεύει ως κεντρικός κόμβος για εγκληματικές πληροφορίες και πληροφορίες·

- υποστηρίζει επιχειρήσεις και έρευνες από τα κράτη μέλη προσφέροντας επιχειρησιακή ανάλυση, συντονισμό και τη σημαντική τεχνογνωσία του·

- παρέχει μια ποικιλία προϊόντων στρατηγικής ανάλυσης που επιτρέπουν τη λήψη τεκμηριωμένων αποφάσεων σε τακτικό και στρατηγικό επίπεδο για την καταπολέμηση και την πρόληψη του εγκλήματος στον κυβερνοχώρο·

- παρέχει μια ολοκληρωμένη λειτουργία προσέγγισης που συνδέει τις αρχές επιβολής του νόμου για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο με τον ιδιωτικό τομέα, τον ακαδημαϊκό κόσμο και άλλους μη εταίρους επιβολής του νόμου·

- υποστηρίζει την κατάρτιση και τη δημιουργία ικανοτήτων, ιδίως για τις αρμόδιες αρχές των κρατών μελών·

- παρέχει εξαιρετικά εξειδικευμένες δυνατότητες τεχνικής και ψηφιακής εγκληματολογικής υποστήριξης σε έρευνες και επιχειρήσεις·

- εκπροσωπεί την κοινότητα επιβολής του νόμου της ΕΕ σε τομείς κοινού ενδιαφέροντος (απαιτήσεις έρευνας και ανάπτυξης, διακυβέρνηση του Διαδικτύου και ανάπτυξη πολιτικών).

(Επίσημος Ιστότοπος του EC3 της Europol, 2022)

2.5 ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΨΗΦΙΑΚΗΣ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑΣ

Σύμφωνα με τα πρόσφατα δημοσιοποιημένα στατιστικά στοιχεία της Ελληνικής αστυνομίας για το έτος 2019 εξιχνιάστηκαν 49.269 αδικήματα οργανωμένου εγκλήματος που αφορούσαν ηλεκτρονικά εγκλήματα και αδικήματα κατά της οικονομίας. Επίσης υπήρξαν συλλήψεις στο σύνολο 198.661 ατόμων συνολικός αριθμός νέων υποθέσεων που έλεγξε η δίωξη ηλεκτρονικού εγκλήματος το έτος 2019 όπου ανήλθε σε αριθμό 5.187. Επιπλέον οι συνεργασίες με τις διεθνείς αστυνομίες για την εξιχνίαση διεθνών εγκλημάτων ανήλθε σε 1.268 συνεργασίες. Τέλος κατά το έτος 2019 για αξιόποινες πράξεις του διαδικτύου συνελήφθησαν συνολικά 39 άτομα εκ των οποίων οι 2 για διεξαγωγή τυχερών παιγνίων, 3 για παραβίαση νομοθεσίας περί της πνευματικής ιδιοκτησίας για απατή με υπολογιστή ,27 για πορνογραφία ανηλίκων, 2 για παραβίαση της εκάστοτε νομοθεσίας για τα προσωπικά δεδομένα, 1 για εξαρτισιογόνες ουσίες ,1 για διακίνηση παράνομων φαρμακευτικών ουσιών, 1 για αρχαιοκαπηλία και τέλος 1 για παράνομη διακίνηση οπλών και εκρηχτικών. Σε αυτό το σημείο είναι σημαντικό να αναφερθεί η μεγάλη συμβολή της Ελληνικής αστυνομίας στην αποτροπή 370 περιπτώσεων εκδήλωσης πρόθεσης αυτοκτονίας μέσω διαδικτύου. Η αστυνομία ωστόσο προτείνει σε κάθε περίπτωση την αναφορά κάθε τέτοιου συμβάντος στην εκαστοτε τοπική αρχή προκειμένου να εξαρθρώνονται εγκαίρως τέτοιες παραβατικές και αποκλίνουσες συμπεριφορές. (Ελληνική αστυνομία , 2021)

Βασικές αξιόποινες πράξεις με την χρήση ψηφιακών μέσων.

2.6 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ ΨΗΦΙΑΚΗ ΑΠΑΤΗ

2.6.1 ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ

Το πρόθεμα «crypto» προέρχεται αρχικά από την ελληνική λέξη που σημαίνει «κρυμμένο». Αυτό δεν σημαίνει ότι το κρυπτονόμισμα είναι μυστικό, αλλά μάλλον ότι αυτά τα «κρυμμένα» χρήματα είναι ψηφιακά και διατηρούνται ασφαλή με κρυπτογράφηση ψηφιακού κώδικα. Αυτά τα ψηφιακά νομίσματα είναι η καρδιά των συστημάτων που επιτρέπουν ασφαλείς, άμεσες πληρωμές για διαδικτυακές συναλλαγές. Το "Crypto-" αναφέρεται στην κρυπτογράφηση δεδομένων που προστατεύει τις συναλλαγές από χάκερ ή άλλες ψηφιακές απειλές. Καθιστά επίσης δύσκολη την παραχάραξη κρυπτονομισμάτων.

Το κρυπτονόμισμα έχει αποκτήσει δημοτικότητα επειδή προσφέρει έναν απλό τρόπο μεταφοράς κεφαλαίων εξ ολοκλήρου διαδικτυακά, χωρίς τη συμμετοχή τρίτων, όπως τράπεζες ή εταιρείες πιστωτικών καρτών (και την πληρωμή των τελών που χρεώνουν συχνά για την επεξεργασία των συναλλαγών). Αντί για φυσικά νομίσματα ή χαρτονομίσματα, τα κρυπτονομίσματα έχουν ψηφιακά «κουπόνια» ή διαφορετικές ψηφιακές ονομαστικές αξίες. Για παράδειγμα, ένα bitcoin ισοδυναμεί με 100.000.000 satoshi, πρόκειται για τη μικρότερη ονομαστική αξία ενός bitcoin και το όνομά του προέρχεται από τον υποτιθέμενο εφευρέτη του bitcoin, Satoshi Nakamoto. Η υποδιαίρεση αυτή επιτρέπει συναλλαγές μικρότερες από ένα πλήρες νόμισμα. Η μεταφορά κεφαλαίων περιλαμβάνει «δημόσια» και «ιδιωτικά» κλειδιά, τα οποία είναι γραμμές κώδικα που πρέπει να ταιριάζουν και στις δύο πλευρές, ώστε η συναλλαγή να μπορεί να ολοκληρωθεί. Το κρυπτονόμισμα αποθηκεύεται στο "πορτοφόλι" του χρήστη, σε μια διεύθυνση URL ή σε μια διεύθυνση λογαριασμού Διαδικτύου στην οποία μπορεί να έχει πρόσβαση μόνο ο κάτοχος. Το πορτοφόλι έχει ένα δημόσιο κλειδί και το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή μιας συναλλαγής, όπως θα υπέγραφε κανείς μια επιταγή ή ένα απόκομμα πιστωτικής κάρτας.

Οι επίδοξοι χρήστες κρυπτονομισμάτων μπορούν να χρησιμοποιήσουν συγκεκριμένους ιστότοπους για να ανταλλάξουν διαφορετικούς τύπους νομισμάτων (όπως ευρώ ή δολάρια) για μάρκες κρυπτονομισμάτων. Το σύστημα που υποστηρίζει κρυπτονομίσματα στο διαδίκτυο ονομάζεται blockchain, το οποίο είναι ουσιαστικά ένα ψηφιακό βιβλίο που παρακολουθεί τις συναλλαγές στο διαδίκτυο. Υπάρχει ένα blockchain για κάθε είδος ψηφιακού κρυπτονομίσματος, το οποίο καταγράφει όλες τις συναλλαγές που χρησιμοποιούν το συγκεκριμένο κρυπτονόμισμα. Αυτό που βοηθά να γίνει το κρυπτονόμισμα μοναδικό είναι ότι δεν υπάρχει κεντρική τράπεζα ή κέντρο επεξεργασίας.

Αντίθετα, το blockchain αποτελείται από την τεχνολογία «κατανεμημένου καθολικού», η οποία είναι μια βάση δεδομένων που μοιράζεται σε ένα δίκτυο τοποθεσιών και διακομιστών. Με τη συμμετοχή μιας συλλογής διαφορετικών δικτύων κατά τη διάρκεια μιας μεταφοράς, δημιουργείται μια ανιχνεύσιμη διαδρομή και μειώνονται οι πιθανότητες να διακοπούν οι συναλλαγές από κυβερνοεπίθεση ή παραβίαση δεδομένων προσθέτοντας

«μάρτυρες» στην πορεία. Διαφορετικοί τύποι κρυπτονομισμάτων (μερικές φορές αναφέρονται και ως "altcoin") περιλαμβάνουν τα bitcoin, Litecoin, Ethereum, Zcash, Dash, Ripple, Monero, NEO, Cardano και EOS. Λόγω της σύγχρονης, τεχνολογικής φύσης των κρυπτονομισμάτων, νέες μορφές εμφανίζονται συνεχώς (Society, 2021).

2.6.2 ΤΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΑ ΚΑΙ Η ΣΧΕΣΗ ΤΟΥΣ ΜΕ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ

Σήμερα τα κρυπτονομίσματα έχουν γίνει ένα παγκόσμιο φαινόμενο γνωστό στους περισσότερους ανθρώπους. Γρήγορα γίνονται mainstream και περισσότεροι άνθρωποι εξερευνούν τον κόσμο των κρυπτογράφησης. Ωστόσο, οι επενδυτές δεν είναι οι μόνοι που ενδιαφέρονται για τα κρυπτονομίσματα - οι εγκληματίες του κυβερνοχώρου ενθουσιάζονται με την ιδέα του μη ελεγχόμενου χρήματος. Άνοιξε νέους φορείς επιθέσεων και έναν νέο τρόπο για τους εγκληματίες του κυβερνοχώρου να εξαφανιστούν χωρίς να αφήνουν ίχνη.

Λόγω της ανώνυμης φύσης τους, τα κρυπτονομίσματα διαδραματίζουν ουσιαστικό ρόλο στην παραοικονομία. Χρησιμοποιούνται για τις περισσότερες πληρωμές από εγκληματίες σε εγκληματίες (C2C) και σε φόρουμ και αγορές του Darknet. Περίπου 76 δισεκατομμύρια δολάρια παράνομης δραστηριότητας ετησίως χρησιμοποιούνται σε Bitcoin και έως το η Cybersecurity Ventures τονίζει ότι περισσότερο από το 70 τοις εκατό όλων των συναλλαγών κρυπτονομισμάτων είναι για παράνομη δραστηριότητα. Επίσης, πολλοί χάκερ απαιτούν πληρωμή από τα θύματα για επιθέσεις, όπως ransomware ή εκβιασμό DDoS, σε κρυπτονομίσματα (V2C – θύμα σε εγκληματία).

Ενώ η άνοδος των κρυπτονομισμάτων διευκολύνει το έγκλημα στον κυβερνοχώρο, γενικά, έδωσε επιπρόσθετα σημαντική ώθηση στην ανάπτυξη νέων τύπων κυβερνοεπιθέσεων. Τα κρυπτονομίσματα έχουν εγγενώς χαμηλά επίπεδα ελέγχου και δεν διέπονται από μια κεντρική αρχή, πράγμα που σημαίνει ότι οι συναλλαγές δεν μπορούν να παρακολουθούνται στενά. Αυτό τα κάνει καταφύγιο για εγκληματικές δραστηριότητες σε όλο τον κόσμο. Οι εγκληματίες μπορούν χρησιμοποιώντας τα κρυπτονομίσματα να μεταφέρουν εύκολα εκατομμύρια δολάρια εκτός συνόρων χωρίς ανίχνευση.

Αρχικά, ούτε οι συναλλαγές ούτε οι λογαριασμοί συνδέονται με ταυτότητες του πραγματικού κόσμου, επομένως είναι εύκολο για τους εγκληματίες του κυβερνοχώρου να παραμένουν αγνώστων στοιχείων όταν χρησιμοποιούν κρυπτογράφηση. Οι πληρωμές γίνονται από "διευθύνσεις Bitcoin" και τα άτομα μπορούν εύκολα να δημιουργήσουν νέες διευθύνσεις. Αν και είναι συνήθως δυνατό να αναλυθεί η ροή των συναλλαγών, δεν είναι εύκολο να συνδεθεί η πραγματική ταυτότητα με τους κατόχους αυτών των διευθύνσεων. Επιπρόσθετα, πρόκειται για συναλλαγές γρήγορες και παγκόσμιες: Οι συναλλαγές κρυπτογράφησης διαδίδονται σχεδόν αμέσως στο δίκτυο και επιβεβαιώνονται σε λίγα

λεπτά. Δεδομένου ότι συμβαίνουν σε ένα παγκόσμιο δίκτυο υπολογιστών, είναι πολύ δύσκολο να προσδιοριστεί η φυσική τοποθεσία.

Τα κρυπτονομίσματα έχουν γίνει τα πιο δημοφιλή μέσα πληρωμής στον σκοτεινό ιστό επειδή επιτρέπουν στους εμπόρους και τους αγοραστές να παραμένουν ανώνυμοι. Εναλλακτικά νομίσματα όπως το Monero και το Verge, τα οποία επικεντρώνονται στο απόρρητο και προσφέρουν ακόμη μεγαλύτερη ανωνυμία από το Bitcoin, έχουν γίνει αγαπημένα για εγκληματικές δραστηριότητες στο Darknet. Υπάρχουν διάφοροι τύποι κυβερνοεπιθέσεων όπου οι κυβερνοεγκληματίες εκμεταλλεύονται τα κρυπτονομίσματα. Περιλαμβάνουν ransomware, εκβιασμό DDoS, cryptojacking και εισβολές ανταλλαγής κρυπτονομισμάτων.

Μία από τις μεγαλύτερες τάσεις εγκλήματος στον κυβερνοχώρο στην ιστορία, το ransomware έχει σχεδιαστεί για να αποσπά χρήματα κρυπτογραφώντας τα δεδομένα των χρηστών. Αυτός ο τύπος κακόβουλου λογισμικού εμφανίζει συνήθως ένα μήνυμα στην οθόνη που προσφέρει την επαναφορά της πρόσβασης αφού το θύμα πληρώσει λύτρα. Συνήθως, οι εγκληματίες του κυβερνοχώρου απαιτούν πληρωμή με τη μορφή Bitcoin ή άλλου ψηφιακού νομίσματος. Έτσι, οι επιτιθέμενοι είναι σχεδόν αδύνατο να εντοπιστούν.

Το 2017 ήταν η μεγαλύτερη χρονιά για επιθέσεις ransomware – παγκόσμιες επιδημίες του περιβόητου WannaCry και NotPetya ransomware που κατέστρεψαν πολλούς μεγάλους οργανισμούς. Το 2017 ήταν επίσης η χρονιά που η τιμή του Bitcoin εκτοξεύτηκε από κάτω από τα 1.000 $ σε σχεδόν 20.000 $, φτάνοντας το ιστορικό υψηλό ποσό των 19.783,21 $ στις 17 Δεκεμβρίου (Allot, 2021) (Δίωξη Ηλεκτρονικού Εγκλήματος, 2022).

2.6.3 ΕΞΑΠΑΤΗΣΗ ΠΟΛΙΤΩΝ ΚΑΤΑ ΤΗΝ ΑΓΟΡΑ ΚΡΥΠΤΟΝΟΜΙΣΜΑΤΩΝ

Σύμφωνα με την Δίωξη Ηλεκτρονικού Εγκλήματος (Δίωξη Ηλεκτρονικού Εγκλήματος, 2022) το τελευταίο διάστημα καταγράφονται περιπτώσεις διεθνούς απάτης που σχετίζονται με υποτιθέμενες επενδύσεις σε κρυπτονομίσματα ή σε επενδυτικά προϊόντα από δημοφιλή, διεθνούς φήμης πρόσωπα, όπως πολιτικοί, ηθοποιοί, τραγουδιστές, επιχειρηματίες κ.α. Πιο συγκεκριμένα, η απάτη συνήθως εκδηλώνεται με την ανάρτηση ψεύτικων ειδήσεων, οι οποίες συνοδεύονται από αντίστοιχο οπτικοακουστικό υλικό, το οποίο υποτίθεται ότι προέρχεται από την ηλεκτρονική έκδοση αναγνωρισμένων εφημερίδων και ιστοτόπων, και σύμφωνα με το οποίο τα διάσημα πρόσωπα φέρονται να έχουν επενδύσει σε κρυπτονομίσματα ή άλλα επενδυτικά προϊόντα καταφέρνοντας σε πολύ μικρό χρονικό διάστημα να αποκομίσουν μεγάλο κέρδος.

Αντίστοιχα, οι αναγνώστες εξαπατώνται με τέτοιο τρόπο ώστε να πράξουν το ίδιο, εισάγοντας τα προσωπικά τους δεδομένα στις δημιουργημένες από τους χάκερς πλατφόρμες επενδύσεων που στοχεύουν στην οικονομική τους εξαπάτηση και την απόσπαση πολύ

σημαντικών ποσών. Στην κατεύθυνση αυτή η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συνιστά στους πολίτες και ιδιαίτερα στους χρήστες του Διαδικτύου:

«Να ελέγχουν την εγκυρότητα των δημοσιευμάτων για επενδυτικά προγράμματα, ακόμα και όταν προβάλλονται ότι συμμετέχουν άτομα με αναγνωρισιμότητα, καθόσον αυτό στοχεύει να πεισθούν διαδικτυακοί χρήστες για την αληθοφάνεια των προβαλλομένων.

Να είναι ιδιαίτερα προσεκτικοί κατά την πλοήγησή τους στο διαδίκτυο και ιδιαίτερα όσον αφορά επενδύσεις με ιδιαίτερα υψηλές και ελκυστικές αποδόσεις.

Να μην ανοίγουν e-mails ή διαφημίσεις που προέρχονται από άτομα που δεν γνωρίζουμε ή δεν περιμένουμε.

Να παραμένουν επιφυλακτικοί όταν τους προσεγγίζουν τηλεφωνικά ή μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου άτομα από επενδυτικές εταιρείες του εξωτερικού και δεν επενδύουμε τα χρήματά μας σε υπηρεσίες χωρίς να είμαστε απολύτως βέβαιοι για την αξιοπιστία τους.

Να διατηρούν επιφυλάξεις αν η προσφορά φαίνεται υπερβολικά καλή για να είναι αληθινή, καθώς και επιφυλάξεις εάν είναι πραγματική. Σκεφτόμαστε δύο φορές πριν κάνουμε κλικ.»

(Δίωξη Ηλεκτρονικού Εγκλήματος, 2021)

ΚΕΦΑΛΑΙΟ 3 – Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR)

3.1 Γενικά για το GDPR

Ο νέος γενικός κανονισμός της ευρωπαϊκής ένωσης 2016/679 του συμβουλίου της 27ης Απριλίου του 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών όπου ορίστηκε άμεση εφαρμογή από όλα τα κράτη μέλη στις 25 Μάιου 2018 αντικατέστησε την υπάρχουσα οδηγία 95/46/ΕΚ και την εθνική νομοθεσία που την ενσωμάτωσε στο νόμο 2472/1997.(Κανελλόπουλος,2018)

3.2 Τι είναι το GDPR;

Ο νέος ευρωπαϊκός νόμος περί απορρήτου και ασφάλειας δεδομένων περιλαμβάνει νέες απαιτήσεις εκατοντάδων σελίδων για οργανισμούς σε όλο τον κόσμο. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) είναι ο πιο σκληρός νόμος περί απορρήτου και ασφάλειας στον κόσμο. Αν και συντάχθηκε και εγκρίθηκε από την

Ευρωπαϊκή Ένωση (ΕΕ), επιβάλλει υποχρεώσεις σε οργανισμούς οπουδήποτε, εφόσον στοχεύουν να ή συλλέγουν δεδομένα που σχετίζονται με άτομα στην ΕΕ. Το GDPR θα επιβάλει σκληρά πρόστιμα σε όσους παραβιάζουν τα πρότυπα απορρήτου και ασφάλειας του, με κυρώσεις που φτάνουν τα δεκάδες εκατομμύρια ευρώ. Με τον GDPR, η Ευρώπη σηματοδοτεί τη σταθερή της θέση για το απόρρητο και την ασφάλεια των δεδομένων σε μια εποχή που περισσότεροι άνθρωποι εμπιστεύονται τα προσωπικά τους δεδομένα σε υπηρεσίες cloud και οι παραβιάσεις είναι καθημερινό φαινόμενο. Ο ίδιος ο κανονισμός είναι μεγάλος, εκτεταμένος και αρκετά ελαφρύς σε ιδιαιτερότητες, καθιστώντας τη συμμόρφωση με τον GDPR μια τρομακτική προοπτική, ιδιαίτερα για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) (Gdpr.eu, 2021).

Gdpr. Eu (2021) What is GDPR, the EU's new data protection law? Διαθέσιμό στο: https://gdpr.eu/what-is-gdpr/

3.2.1 Ιστορία του GDPR

Το δικαίωμα στην ιδιωτική ζωή είναι μέρος της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα του 1950, η οποία ορίζει: «Καθένας έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, του σπιτιού του και της αλληλογραφίας του». Από αυτή τη βάση, η Ευρωπαϊκή Ένωση επιδίωξε να διασφαλίσει την προστασία αυτού του δικαιώματος μέσω νομοθεσίας. Καθώς η τεχνολογία προχωρούσε και εφευρέθηκε το Διαδίκτυο, η ΕΕ αναγνώρισε την ανάγκη για παροχή σύγχρονης προστασίας. Έτσι, το 1995 ψήφισε την Ευρωπαϊκή Οδηγία για την Προστασία Δεδομένων, καθιερώνοντας ελάχιστα πρότυπα απορρήτου και ασφάλειας δεδομένων, στα οποία κάθε κράτος μέλος βασίζει τον δικό του εκτελεστικό νόμο. Αλλά ήδη το Διαδίκτυο μεταμορφωνόταν στα δεδομένα που είναι σήμερα. Το 1994, η πρώτη διαφήμιση banner εμφανίστηκε στο διαδίκτυο. Το 2000, η πλειονότητα των χρηματοπιστωτικών ιδρυμάτων προσέφεραν διαδικτυακή τραπεζική. Το 2006, το Facebook άνοιξε στο κοινό. Το 2011, ένας χρήστης της Google μήνυσε την εταιρεία για σάρωση των email της. Δύο μήνες μετά από αυτό, η αρχή προστασίας δεδομένων της Ευρώπης δήλωσε ότι η ΕΕ χρειαζόταν «μια συνολική προσέγγιση για την προστασία των προσωπικών δεδομένων» και άρχισαν οι εργασίες για την ενημέρωση της οδηγίας του 1995. Ο GDPR τέθηκε σε ισχύ το 2016 μετά την ψήφιση του Ευρωπαϊκού Κοινοβουλίου και από τις 25 Μαΐου 2018, όλοι οι οργανισμοί έπρεπε να συμμορφωθούν(Gdpr.eu,2021).

3.3 Πεδίο εφαρμογής, ποινές και βασικοί ορισμοί

Πρώτον, εάν επεξεργάζεστε προσωπικά δεδομένα πολιτών ή κατοίκων της ΕΕ ή προσφέρετε αγαθά ή υπηρεσίες σε τέτοια άτομα, τότε ο GDPR είναι σε ισχύ ακόμη κι αν δεν βρίσκεστε στην ΕΕ. Δεύτερον, τα πρόστιμα για παραβίαση του GDPR είναι πολύ υψηλά. Υπάρχουν δύο βαθμίδες κυρώσεων, οι οποίες ανέρχονται στο μέγιστο των 20 εκατομμυρίων ευρώ ή στο 4% των παγκόσμιων εσόδων (όποιο είναι υψηλότερο), συν τα υποκείμενα των δεδομένων έχουν το δικαίωμα να ζητήσουν αποζημίωση για ζημίες. Αυτά πρόκειται για πρόστιμα GDPR (Gdpr.eu, 2021). Ο GDPR ορίζει εκτενώς μια σειρά νομικών όρων που αναφέρονται ως ακολούθως:

3.3.1 Προσωπικά δεδομένα

Προσωπικά δεδομένα είναι κάθε πληροφορία που σχετίζεται με ένα άτομο που μπορεί να αναγνωριστεί άμεσα ή έμμεσα. Τα ονόματα και οι διευθύνσεις ηλεκτρονικού ταχυδρομείου είναι προφανώς προσωπικά δεδομένα. Πληροφορίες τοποθεσίας, εθνικότητα, φύλο, βιομετρικά δεδομένα, θρησκευτικές πεποιθήσεις, cookies ιστού και πολιτικές απόψεις μπορεί επίσης να είναι προσωπικά δεδομένα. Τα ψευδώνυμα δεδομένα μπορούν επίσης να εμπίπτουν στον ορισμό, εάν είναι σχετικά εύκολο να αναγνωριστεί κάποιος από αυτά (Gdpr.eu, 2021).

3.3.2 Επεξεργασία δεδομένων

Επεξεργασία δεδομένων λογίζεται η οποιαδήποτε ενέργεια εκτελείται σε δεδομένα, είτε είναι αυτοματοποιημένη είτε μη αυτόματη. Τα παραδείγματα που αναφέρονται στο κείμενο περιλαμβάνουν τη συλλογή, την καταγραφή, την οργάνωση, τη δομή, την αποθήκευση, τη χρήση, τη διαγραφή επομένως το οτιδήποτε (Gdpr.eu, 2021).

3.3.3 Υποκείμενο δεδομένων

Υποκείμενο δεδομένων είναι το πρόσωπο του οποίου τα δεδομένα υποβάλλονται σε επεξεργασία. Αυτά τα υποκείμενα είναι οι πελάτες ή οι επισκέπτες του ιστότοπού (Gdpr.eu, 2021).

3.3.4 Υπεύθυνος επεξεργασίας δεδομένων

Ως υπεύθυνος επεξεργασίας δεδομένων ορίζεται το άτομο που αποφασίζει το λόγο και τον τρόπο που θα πραγματοποιηθεί η επεξεργασία των προσωπικών δεδομένων και είναι πιθανό να πρόκειται για ιδιοκτήτη ή υπάλληλο στην επιχείρηση που χειρίζεται τα δεδομένα. Ο υπεύθυνος επεξεργασίας δεδομένων μπορεί να είναι και ένα τρίτο μέρος που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό υπεύθυνου επεξεργασίας δεδομένων. Ο GDPR έχει ειδικούς κανόνες για αυτά τα άτομα και τους οργανισμούς. Θα μπορούσαν να περιλαμβάνουν διακομιστές cloud όπως το Tresorit ή παρόχους υπηρεσιών email όπως το ProtonMail (Gdpr.eu, 2021).

3.4 Το GDPR και τα βασικά ρυθμιστικά σημεία του GDPR.

3.4.1 Αρχές προστασίας δεδομένων

Εάν πραγματοποιείται η επεξεργασία δεδομένων, πρέπει να πραγματοποιείται σύμφωνα με επτά αρχές προστασίας και λογοδοσίας που περιγράφονται ως ακολούθως.

Στο άρθρο 5.1-2 περιγράφονται τα εξής:

1. Νομιμότητα, δικαιοσύνη και διαφάνεια

Η επεξεργασία πρέπει να είναι νόμιμη, δίκαιη και διαφανής για το υποκείμενο των δεδομένων.

2. Περιορισμός σκοπού

Πρέπει να επεξεργάζεστε δεδομένα για τους νόμιμους σκοπούς που προσδιορίζονται ρητά στο υποκείμενο των δεδομένων όταν συλλέγονται (Gdpr.eu, 2021).

3. Ελαχιστοποίηση δεδομένων

Θα πρέπει να συλλέγονται και να επεξεργάζονται μόνο όσα δεδομένα είναι απολύτως απαραίτητα για τους καθορισμένους σκοπούς (Gdpr.eu, 2021).

4. Ακρίβεια

Πρέπει να διατηρούνται τα προσωπικά δεδομένα ακριβή και ενημερωμένα (Gdpr.eu, 2021).

5. Περιορισμός αποθήκευσης

Μπορείτε να αποθηκεύονται δεδομένα προσωπικής ταυτοποίησης μόνο για όσο διάστημα είναι απαραίτητο για τον καθορισμένο σκοπό (Gdpr.eu, 2021).

6. Ακεραιότητα και εμπιστευτικότητα

Η επεξεργασία πρέπει να γίνεται με τέτοιο τρόπο ώστε να διασφαλίζεται η κατάλληλη ασφάλεια, ακεραιότητα και εμπιστευτικότητα (π.χ. με χρήση κρυπτογράφησης) (Gdpr.eu, 2021).

7. Υπευθυνότητα

Ο υπεύθυνος επεξεργασίας δεδομένων είναι υπεύθυνος να μπορεί να αποδείξει τη συμμόρφωση με τον GDPR με όλες αυτές τις αρχές (Gdpr.eu, 2021).

3.4.2 Ευθύνη

Σύμφωνα με το GDPR οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να είναι σε θέση να αποδείξουν ότι συμμορφώνονται με τον GDPR. Και αυτό δεν είναι κάτι που μπορεί να γίνει εκ των υστέρων. Εάν υπάρχει η θεώρηση της συμμόρφωσης με τον GDPR δίχως να υπάρχει η δυνατότητα επίδειξής της τότε δεν υπάρχει συμμόρφωση με τον GDPR (Gdpr.eu, 2021).

Οι τρόποι που μπορεί να αποδείξουν συμμόρφωση περιγράφονται παρακάτω:

• Θα πρέπει να οριστούν ευθύνες προστασίας δεδομένων στην ομάδα εργασίας.

• Θα πρέπει να διατηρείται λεπτομερής τεκμηρίωση των δεδομένων που συλλέγονται, πώς χρησιμοποιούνται, πού αποθηκεύονται, ποιος υπάλληλος είναι υπεύθυνος για αυτά κ.λπ (Gdpr.eu, 2021).

• Θα πρέπει να υπάρχει εκπαίδευση του προσωπικού και να εφαρμόζονται τεχνικά και οργανωτικά μέτρα ασφαλείας (Gdpr.eu, 2021).

• Θα πρέπει να συνάπτονται συμβάσεις Συμφωνίας Επεξεργασίας Δεδομένων με τρίτα μέρη τα οποία θα πραγματοποιούν την επεξεργασία δεδομένων για λογαριασμό της επιχείρησης (Gdpr.eu, 2021).

• Είναι απαραίτητο να διοριστεί ένας Υπεύθυνος Προστασίας Δεδομένων (αν και δεν χρειάζονται όλες οι επιχειρήσεις) (Gdpr.eu, 2021).

3.4.3 Ασφάλεια δεδομένων

Απαιτείται ο χειρισμός των δεδομένων με ασφάλεια εφαρμόζοντας «κατάλληλα τεχνικά και οργανωτικά μέτρα». Τα τεχνικά μέτρα σημαίνουν οτιδήποτε, από την απαίτηση από τους υπαλλήλους σας να χρησιμοποιούν έλεγχο ταυτότητας δύο παραγόντων σε λογαριασμούς όπου αποθηκεύονται προσωπικά δεδομένα έως τη σύναψη συμβάσεων με παρόχους cloud που χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο. Τα οργανωτικά μέτρα αφορούν ζητήματα όπως η εκπαίδευση του προσωπικού, η προσθήκη μιας πολιτικής απορρήτου δεδομένων στο εγχειρίδιο υπαλλήλων ή ο περιορισμός της πρόσβασης στα προσωπικά δεδομένα μόνο σε εκείνους τους υπαλλήλους του οργανισμού που τους είναι απαραίτητο. Εάν υπάρχει παραβίαση δεδομένων, το χρονικό περιθώριο είναι 72 ώρες για να ενημερωθούν τα υποκείμενα των δεδομένων, διαφορετικά θα αντιμετωπιστούν κυρώσεις. (Αυτή η απαίτηση ειδοποίησης μπορεί να παραλειφθεί εάν χρησιμοποιούνται τεχνολογικές διασφαλίσεις, όπως η κρυπτογράφηση, για να καταστηθούν άχρηστα δεδομένα σε έναν εισβολέα) (Gdpr.eu, 2021).

3.4.4 Προστασία δεδομένων από σχεδιασμό και από προεπιλογή

Ότι γίνετε στον οργανισμό πρέπει, «από το σχεδιασμό και από προεπιλογή» να εξετάζεται σύμφωνα με την προστασία δεδομένων. Πρακτικά, αυτό σημαίνει ότι πρέπει να ληφθούν υπόψη οι αρχές προστασίας δεδομένων κατά το σχεδιασμό οποιουδήποτε νέου προϊόντος ή δραστηριότητας. Ο GDPR καλύπτει αυτήν την αρχή στο άρθρο 25. Επ' αυτού τίθεται η υπόθεση, για παράδειγμα, ότι ξεκινάει μια νέα εφαρμογή για την εταιρεία. Πρέπει να τεθεί επί τάπητος ποια προσωπικά δεδομένα θα μπορούσαν ενδεχομένως να συλλεχθούν από την εφαρμογή από τους χρήστες, στη συνέχεια να εξεταστούν οι τρόποι για την ελαχιστοποίηση του όγκου των δεδομένων και πώς θα προστατευθούν με την τελευταία λέξη της τεχνολογίας (Gdpr.eu, 2021).

3.4.5. Άδεια επεξεργασίας δεδομένων

Το άρθρο 6 απαριθμεί τις περιπτώσεις στις οποίες είναι νόμιμη η επεξεργασία δεδομένων προσώπων. Δεν θα πρέπει να υπάρχει η ενασχόληση με τα προσωπικά δεδομένα κάποιου που σημαίνει ότι δεν θα πρέπει να συλλέγονται, να αποθηκεύονται, να πωλούνται σε διαφημιστές - εκτός εάν είναι εφικτή η αιτιολογία χρησιμοποιώντας ένα από τα ακόλουθα επιχειρήματα (Gdpr.eu, 2021):

1. Το υποκείμενο των δεδομένων δίνει συγκεκριμένη, ξεκάθαρη συγκατάθεση για την επεξεργασία των δεδομένων. Για παράδειγμα τα υποκείμενα έχουν επιλέξει από μόνα τους να συμμετέχουν στη λίστα email μάρκετινγκ) (Gdpr.eu, 2021).

2. Η επεξεργασία είναι απαραίτητη για την εκτέλεση ή την προετοιμασία για τη σύναψη σύμβασης στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος. Παραδείγματος χάριν, πρέπει να γίνει έλεγχος ιστορικού πριν ολοκληρωθεί η εκμίσθωση ακινήτου σε υποψήφιο ενοικιαστή (Gdpr.eu, 2021).

3. Πρέπει να γίνει επεξεργασία για τη συμμόρφωση με μια νομική υποχρέωση. Αυτό σημαίνει ότι λαμβάνετε εντολή από το δικαστήριο της δικαιοδοσίας (Gdpr.eu, 2021).

4. Πρέπει να γίνεται επεξεργασία των δεδομένων για να σωθεί η ζωή κάποιου που κινδυνεύει. Για παράδειγμα πιθανότατα να είναι γνωστό το πότε πρέπει να ισχύει αυτό) (Gdpr.eu, 2021)

5. Η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας αποστολής προς το δημόσιο συμφέρον ή για την εκτέλεση κάποιας επίσημης λειτουργίας. Για παράδειγμα μια ιδιωτική εταιρεία συλλογής σκουπιδιών) (Gdpr.eu, 2021).

6. Υπάρχει έννομο συμφέρον για την επεξεργασία των προσωπικών δεδομένων κάποιου. Αυτή είναι η πιο ευέλικτη νόμιμη βάση, αν και τα «θεμελιώδη δικαιώματα και ελευθερίες του υποκειμένου των δεδομένων» υπερισχύουν πάντα των συμφερόντων, ειδικά εάν πρόκειται για δεδομένα παιδιού (Gdpr.eu, 2021).

Στην προκείμενη περίπτωση είναι δύσκολο να δοθεί ένα παράδειγμα εδώ επειδή υπάρχουν διάφοροι παράγοντες που θα πρέπει να ληφθούν υπόψη για τη συγκεκριμένη περίπτωσή. Αφού πραγματοποιηθεί προσδιορισμός της νόμιμης βάσης για την επεξεργασία των δεδομένων, πρέπει να τεκμηριωθεί αυτή η βάση και να ενημερωθεί το υποκείμενο των δεδομένων ώστε να υπάρχει διαφάνεια!. Και αν ληφθεί η απόφαση αργότερα για αλλαγή της αιτιολόγησής, πρέπει να υπάρχει ένας καλός λόγος, να είναι τεκμηριωμένος και να ενημερωθεί το υποκείμενο των δεδομένων (Gdpr.eu, 2021).

3.4.6. Συγκατάθεση

Υπάρχουν αυστηροί νέοι κανόνες σχετικά με το τι συνιστά συγκατάθεση ενός υποκειμένου των δεδομένων για την επεξεργασία των πληροφοριών του (Gdpr.eu, 2021).

• Η συγκατάθεση πρέπει να «δίδεται ελεύθερα, να είναι συγκεκριμένη, ενημερωμένη και ξεκάθαρη».

• Τα αιτήματα για συναίνεση πρέπει να είναι «ξεκάθαρα διακριτά από τα άλλα θέματα» και να παρουσιάζονται σε «σαφή και απλή γλώσσα».

• Τα υποκείμενα των δεδομένων μπορούν να αποσύρουν τη συγκατάθεσή τους όποτε θέλουν και πρέπει να τηρήσουν την απόφασή τους. Δεν είναι εφικτό να αλλαχθεί η νομική βάση της επεξεργασίας σε μία από τις άλλες αιτιολογήσεις.

• Παιδιά κάτω των 13 ετών μπορούν να δώσουν τη συγκατάθεσή τους μόνο με την άδεια του γονέα τους.

• Πρέπει να διατηρούνται αποδεικτικά έγγραφα συγκατάθεσης (Gdpr.eu, 2021).

3.4.7 Υπεύθυνοι Προστασίας Δεδομένων

Σε αντίθεση με τη δημοφιλή πεποίθηση, δεν χρειάζεται κάθε υπεύθυνος επεξεργασίας δεδομένων να διορίζει Υπεύθυνο Προστασίας Δεδομένων (DPO) (Gdpr.eu, 2021).

Υπάρχουν τρεις προϋποθέσεις υπό τις οποίες απαιτείται να οριστεί ένας Υπεύθυνος Προστασίας Δεδομένων:

1. Όταν πρόκειται για δημόσια αρχή διαφορετική από δικαστήριο που ενεργεί υπό δικαστική ιδιότητα.

2. Οι βασικές δραστηριότητες απαιτούν τη συστηματική και τακτική παρακολούθηση ανθρώπων σε μεγάλη κλίμακα. (για παράδειγμα όπως η Google.)

3. Οι κύριες δραστηριότητές είναι η μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 του GDPR ή δεδομένων που σχετίζονται με ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10. (για παράδειγμα όταν πρόκειται για ιατρείο) (Gdpr.eu, 2021).

Θα μπορούσε επίσης να επιλεγεί ο ορισμός ενός Υπευθύνου Προστασίας Δεδομένων ακόμα κι αν δεν είναι απαραίτητο. Υπάρχουν οφέλη με την αξιοποίηση ενός ατόμου σε αυτή τη θέση. Τα βασικά καθήκοντα περιλαμβάνουν την κατανόηση του GDPR και του τρόπου εφαρμογής του στον οργανισμό, την παροχή συμβουλών σε άτομα του οργανισμού σχετικά με τις ευθύνες τους, τη διεξαγωγή εκπαιδεύσεων για την προστασία δεδομένων, τη διενέργεια ελέγχων και την παρακολούθηση της συμμόρφωσης με το GDPR και την υπηρεσία ως σύνδεσμο με τις ρυθμιστικές αρχές (Gdpr.eu, 2021).

3.4.8 Δικαιώματα απορρήτου των ανθρώπων

Είτε έχοντας της θέση του υπεύθυνου επεξεργασίας δεδομένων ή/και το άτομο είναι υπεύθυνο επεξεργασίας δεδομένων που χρησιμοποιεί το Διαδίκτυο, λογίζεται συνάμα και

ως υποκείμενο δεδομένων. Ο GDPR αναγνωρίζει μια σειρά από νέα δικαιώματα απορρήτου για τα υποκείμενα των δεδομένων, τα οποία στοχεύουν να δώσουν στα άτομα περισσότερο έλεγχο των δεδομένων που δανείζουν σε επιχειρήσεις. Ως επιχείρηση, είναι σημαντικό να κατανοηθεί ότι αυτά τα δικαιώματα για να διασφαλιστούν ότι υπάρχει συμμόρφωση με τον GDPR. Ακολουθεί μια σύνοψη των δικαιωμάτων απορρήτου των υποκειμένων των δεδομένων:

1. Δικαίωμα ενημέρωσης

2. Το δικαίωμα πρόσβασης

3. Δικαίωμα διόρθωσης

4. Δικαίωμα διαγραφής

5. Δικαίωμα περιορισμού της επεξεργασίας

6. Δικαίωμα φορητότητας δεδομένων

7. Δικαίωμα αντίρρησης

8. Δικαιώματα σε σχέση με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ.

Βασικά στοιχεία του GDRP. Πηγή: britishrowing.org

3.5 ΥΠΕΥΘΥΝΟΙ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Οι υπεύθυνοι επεξεργασίας των προσωπικών δεδομένων πρέπει να εφαρμόζουν κατάλληλα μέτρα για την εφαρμογή του κανονισμού. Οι διαδικασίες που σχετίζονται με τα επιχειρηματικά ζητήματα χρησιμοποιούν προσωπικά δεδομένα πρέπει να κατασκευάζονται με βάση τους κανόνες και να παρέχουν εγγύηση για την προστασία των δεδομένων παράδειγμα η χρήση κάποιου ψευδωνύμου ή κι τελείως ανώνυμος όπου χρειάζεται. (Θεματολογικά δελτία για την Ευρωπαϊκή ένωση, 2021)

Οι υπεύθυνοι επεξεργασίας των δεδομένων πρέπει όταν σχεδιάζουν πληροφοριακά συστήματα να βασίζονται στην διαδικασία του απορρήτου με την χρήση όσο των δυνατόν υψηλότερων ρυθμίσεων του απορρήτου έτσι ώστε σχεδόν καμία από τις πληροφορίες να μην είναι δημόσιες και να μην μπορούν να χρησιμοποιηθούν για την αναγνώριση ενός θέματος. Η επεξεργασία προσωπικών δεδομένων απαγορεύεται εκτός και αν συγκαταλέγεται στις εξής νόμιμες βάσεις που καθορίζονται από τον κανονισμό(συγκατάθεση ,σύμβαση, ζωτικό συμφέρον ,νόμιμο συμφέρον- νομική απαίτηση).Όταν η επεξεργασία γίνεται σύμφωνα με την έγκριση του ιδιοκτήτη (συγκατάθεση) το υποκείμενο των δεδομένων έχει το δικαίωμα να ανακαλεστεί ανά πάσα στιγμή. Επιπλέον ,οι υπεύθυνοι επεξεργασίας των δεδομένων σε οποιαδήποτε διαδικασία συλλογής δεδομένων πρέπει να αποτυπώνουν την νόμιμη βάση και τον λόγο της επεξεργασίας αυτών, έπειτα να δηλώνουν για πόσο διάστημα διατηρούνται τα δεδομένα ή εάν κοινοποιούνται σε τρίτους ή εκτός της ευρωπαϊκής ένωσης .Οι μεγάλες πολυεθνικές εταιρίες είναι υποχρεωμένες για την προστασία των δεδομένων των υπαλλήλων και σε ορισμένες περιπτώσεις των καταναλωτών τους στον βαθμό των μόνο απαραίτητων δεδομένων έτσι ώστε να δίνεται η ελάχιστη επεξεργασία από ξένα άτομα. (Θεματολογικά δελτία για την Ευρωπαϊκή ένωση, 2021)

3.6.1 ΕΞΑΙΡΕΣΕΙΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Ορισμένες καταστάσεις δεν υπάγονται στον κανονισμό της προστασίας προσωπικών δεδομένων. Αυτές είναι οι προσωπικές ή οικιακές δραστηριότητες , η εθνική ασφάλεια και τέλος η επιβολή του νόμου. Ο κανονισμός δημιουργήθηκε αποκλειστικά για την ρύθμιση των προσωπικών δεδομένων που διαχειρίζονται οι εταιρίες. Αυτό που δεν χειρίζεται ο κανονισμός είναι η μη εμπορικές πληροφορίες ή οι δραστηριότητες των νοικοκυριών .Ένα παράδειγμα οικιακής δραστηριότητας είναι η αποστολή ενός μηνύματος μεταξύ δυο συγγενικών προσώπων. Επιπροσθέτως , ο κανονισμός δεν ισχύει όταν τα δεδομένα προορίζονται για αστυνομικούς λόγους. Τέλος , μια επιχείρηση για να συμμετέχει στον

κανονισμό για την προστασία προσωπικών δεδομένων πρέπει να έχει την λεγόμενη οικονομική δραστηριότητα.

3.7 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

Ο κανονισμός εφαρμόζεται από τον υπεύθυνο επεξεργασία δεδομένων ο οποίος θεωρείται ότι είναι ένας οργανισμός που συλλέγει δεδομένα από κατοίκους της Ευρωπαϊκής ένωσης ή από έναν μεσολαβητή όπου είναι ένας οργανισμός που συλλέγει δεδομένα για τον υπεύθυνο επεξεργασίας των δεδομένων όπως οι υπηρεσίες ηλεκτρονικής αποθήκευσης σε κοινόχρηστες βάσεις δεδομένων. Σε ορισμένες περιπτώσεις ο κανονισμός εφαρμόζεται σε οργανισμούς που έχουν έδρα εκτός Ευρωπαϊκής ένωσης εάν συλλέγουν ή επεξεργάζονται προσωπικά στοιχεία ατόμων που βρίσκονται εντός Ευρωπαϊκής ένωσης. Η ευρωπαϊκή επιτροπή ορίζει ότι τα προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία που αφορά ένα άτομο είτε σχετίζεται με την ιδιωτική, επαγγελματική ή δημόσια ζωή του. Μπορεί να είναι οτιδήποτε από ένα απλό όνομα ,μια διεύθυνση κατοικίας ,λεπτομέρειες τραπέζης ,αναρτήσεις σε ιστότοπους κοινωνικής δικτύωσης ή ακόμα και προσωπικές ιατρικές πληροφορίες.

Στον κανονισμό επίσης ορίζεται ότι σε οποιαδήποτε απόφαση διοικητικής ή δικαστικής δομής που απαιτεί από τον υπεύθυνο επεξεργασίας ή τον μεταποίητή να αποκαλύψει με τον οποιονδήποτε τρόπο προσωπικά δεδομένα η παρούσα εντολή δεν μπορεί να αναγνωριστεί ή να εκτελεστεί εκτός και αν έχει υπογραφεί κάποια διεθνή συμφωνία ή κάποιο συμβόλαιο δικαστικής συνδρομής εντός και εκτός Ευρωπαϊκής ένωσης. Σε όλα τα κράτη μέλη θα πρέπει να υπάρχει μια εποπτεύουσα αρχή η οποία θα είναι ανεξάρτητη για την ακρόαση και την ερεύνηση καταγγελιών και σε περίπτωση παραβίασης να ασκούνται οι αντίστοιχες κυρώσεις. Οι παραπάνω ανεξάρτητες αρχές θα πρέπει να συνεργάζονται και με άλλες ανεξάρτητες αρχές των κρατών μελών για την παροχή αμοιβαίας βοήθειας.

(lawspot/gdpr, 2018)

3.8 ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΒΟΛΗΣ ΚΥΡΩΣΕΩΝ ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΑΡΑΒΙΑΣΗΣ

Σύμφωνα με τον κανονισμό προστασίας προσωπικών δεδομένων στο κεφάλαιο VIII ¨προσφυγές ευθύνη και κυρώσεις¨ στο άρθρο 83 όπου ορίζονται γενικοί όροι επιβολής διοικητικών προστίμων ορίζουν τα κάτωθι.

1. Κάθε εποπτική αρχή φροντίζει ώστε η επιβολή διοικητικών προστίμων σύμφωνα με το συγκεκριμένο άρθρο έναντι παραβάσεων του συγκεκριμένου κανονισμού όπου ορίζονται στα προηγούμενα άρθρα να είναι για κάθε μεμονωμένη αποτελεσματική και αποτρεπτική. Ανάλογα με τις περιστάσεις τα πρόστιμα ορίζονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος

2. Κατά την λήψη της απόφασης σχετικά με την επιβολή διοικητικού προστίμου για κάθε περίπτωση λαμβάνονται υπόψη τα παρακάτω

α)η φύση, η βαρύτητα, η διάρκεια της παράβασης έχοντας υπόψη την φύση, την έκταση, τον σκοπό της σχετικής επεξεργασίας αλλά και τον αριθμό των υποκείμενων δεδομένων που επηρέασε η παράβαση αλλά και τον βαθμό ζημιάς που υπέστησαν

β)ο δόλος ή η αμέλεια που προκάλεσε την παράβαση

γ) οποιαδήποτε ενέργεια στην οποία επενέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για να μειώσει την ζημιά που υπέστησαν τα υποκείμενα των δεδομένων

δ) ο βαθμός ευθύνης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία λαμβάνοντας υπόψη τεχνικά και οργανωτικά μέτρα

ε) τυχόν σχετικές προηγούμενες παραβάσεις του υπευθύνου επεξεργασίας ή του εκτελούντα την επεξεργασία

στ)ο βαθμός συνεργασίας με την αρχή ελέγχου για την επανόρθωση της παράβασης και τον περιορισμό των πιθανών αρνητικών επιπτώσεων της

ζ) η κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει την παράβαση

η) ο τρόπος με τον οποίο η εποπτική αρχή πληροφορήθηκε της παραβάσεως ειδικά εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία κοινοποιήσει την παράβαση

θ) η τήρηση εγκεκριμένων κωδικών δεοντολογίας σύμφωνα με το άρθρο 40 ή εγκεκριμένων μηχανισμών πιστοποίησης σύμφωνα με το άρθρο 42

ι) κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο που προκύπτει από τις περιστάσεις της συγκεκριμένης περίπτωσης όπως οικονομικά οφέλη που εισπράχθηκαν ή ζημίες που αποφεύχθηκαν άμεσα ή έμμεσα από την παράβαση.

Στην συνέχεια σε περίπτωση που ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για συγκεκριμένες πράξεις επεξεργασίας παραβιάζει αρκετές διατάξεις του παρόντος κανονισμού το συνολικό ποσό του διοικητικού προστίμου δεν υπερβαίνει το ποσό που ορίζεται για την βαρύτερη παράβαση. Επι προσθέτος παραβάσεις των παρακάτω διατάξεων σύμφωνα με την παράγραφο 2 λαμβάνουν διοικητικά πρόστιμα έως 10.000.000 ευρώ ή σε περίπτωση επιχειρήσεων έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους ανάλογα με τον ποιο είναι υψηλότερο ,οι υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία σύμφωνα με τα άρθρα 8,11,25.

Επιπλέον, οι παραβάσεις που περιλαμβάνουν τις βασικές αρχές για την επεξεργασία συμπεριλαμβανομένου τον όρο που ισχύει για την έγκριση τα δικαιώματα των υποκείμενων και των δεδομένων αλλά και την διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτη σε τρίτη χώρα ή σε διεθνή οργανισμό και τέλος την μη συμμόρφωση προς εντολή ή προς προσωρινό ή οριστικό περιορισμό της επεξεργασίας ή προς αναστολή κυκλοφορίας δεδομένων που επιβάλει η εποπτική αρχή και η μη παροχή πρόσβασης κατά παράβαση επισύρουν διοικητικά πρόστιμα έως 20.000.000 ευρώ ή σε περίπτωση επιχειρήσεων έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου έτους ανάλογα με το ποιο είναι υψηλότερο.

Εν συνεχεία, η άσκηση εκ μέρους της εποπτικής αρχής των εξουσιών της δυνάμει του παρόντος άρθρου υπόκειται στις δέουσες δικονομικές εγγυήσεις σύμφωνα με το δίκαιο της Ευρωπαϊκής ένωσης και το δίκαιο του κράτους μέλους συμπεριλαμβανομένου της άσκησης δικαστικής προσφυγής και της τήρησης της παραπάνω διαδικασίας.

Αξίζει να σημειωθεί επιπλέον ότι σύμφωνα με το άρθρο 84 που αναφέρεται στις κυρώσεις λογίζεται ότι τα κράτη μέλη θεσπίζουν τους κανόνες σχετικά με τις άλλες κυρώσεις που επιβάλλονται για παραβάσεις του συγκεκριμένου κανονισμού ιδίως για τις παραβάσεις που δεν αποτελούν κομμάτι των διοικητικών προστίμων και λαμβάνουν όλα τα αναγκαία μέτρα δια ασφαλίσεως της εφαρμογής τους αρκεί η εν λόγο κυρώσεις να είναι αποτελεσματικές αναλογικές και αποτρεπτικές

(Επίσημη εφημερίδα της Ευρωπαϊκής ένωσης, 2016)

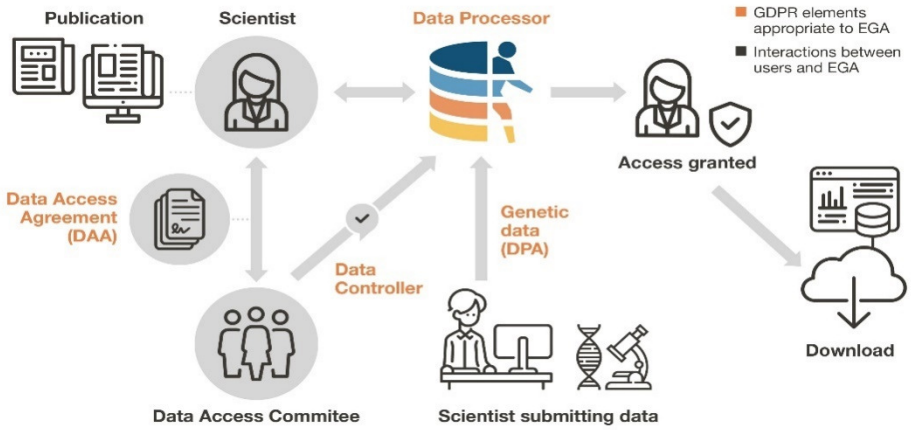
3.9 Ο ΡΟΛΟΣ ΤΟΥ GDPR ΣΤΗΝ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΨΗΦΙΑΚΗ ΠΑΡΑΒΑΤΙΚΟΤΗΤΑ

Στις επιχειρήσεις ο γενικός κανονισμός προστασίας προσωπικών δεδομένων επιφέρει ορισμένα πλεονεκτήματα αλλά και κάποιες δυσκολίες στην εφαρμογή του. Αρχικά, στην κατηγορία των δυσκολιών υπάρχει πρόβλημα στην αποθήκευση ,οργάνωση και ανάκτηση των δεδομένων. Σύμφωνα με μια μελέτη της εταιρίας talent το έτος 2018 συμμετείχαν συνολικά 103 επιχειρήσεις οι οποίες είτε λειτουργούσαν είτε η έδρα τους βρίσκονταν στην Ευρώπη και δραστηριοποιούταν σε πολλούς κυρίαρχους κλάδους της αγοράς. Το αποτέλεσμα της έρευνας ήταν ότι υπήρξαν προβλήματα στην εκτέλεση των δυο κυρίαρχων άρθρων του κανονισμού του άρθρου 15 δικαίωμα πρόσβασης με βάση το θέμα των δεδομένων αλλά και του άρθρου 20 δικαίωμα στην φορητότητα των δεδομένων. Ενώ η πλειοψηφία των επιχειρήσεων καταλάβαινε την σημασία του κανονιστικού πλαισίου της προστασίας προσωπικών δεδομένων το αρνητικό σημείο βρίσκονταν σε ότι αφορά τις εξελιγμένες τεχνολογίες που χρειαζόντουσαν για την επεξεργασία μεγάλου εύρους δεδομένων με αποτέλεσμα οι επιχειρήσεις αυτές σε αρκετές περιπτώσεις να έχουν προβλήματα στην διαρροή προσωπικών δεδομένων σύμφωνα με αυτά που ορίζει ο νέος κανονισμός. Επιπλέον, σύμφωνα με την ίδια έρευνα η επιχειρήσεις που δραστηριοποιούνται στο λιανεμπόριο εμφάνισαν τα χαμηλότερα ποσοστά συμμέτοχης στον νέο κανονισμό σε σχέση με τις πολυεθνικές . Συγκεκριμένα το 76 % των επιχειρήσεων οι οποίες δραστηριοποιούνται στον τομέα του λιανεμπορίου απέτυχαν να ενταχθούν στον κανονισμό. Εξαιτίας της μεγάλης νομικής αλλά και υλικής υποδομής που χρειάζονται για να ενταχθεί μια επιχείρηση στον συγκεκριμένο κανονισμό δυστυχώς με μεγάλη δυσκολία το ποσοστό επιτυχίας έφτασε μόνο το 50%.(Μαρκέτος , 2018)

Παρόλα αυτά υπάρχουν και τα θετικά στοιχεία της συμβολής του κανονισμού ως προς τις επιχειρήσεις καθώς ο κανονισμός προστατεύει σε μεγάλο βαθμό και ειδικά τις πολυεθνικές επιχειρήσεις που διαχειρίζονται μεγάλο όγκο δεδομένων. Επιπλέον βοηθάει στην διαχείριση πολλών στοιχείων με μεγαλύτερη επιμέλεια αφού υπάρχουν ειδικοί υπεύθυνοι επεξεργασίας και υπεύθυνοι εκτελούντων την επεξεργασία αλλά και υπεύθυνος προστασίας δεδομένων όπου ελέγχει συνεχώς την ορθότητα τήρησης του κανονισμού αλλά και την διαχείριση διαφόρων δραστηριοτήτων που αφορούν τα προσωπικά δεδομένα όπως η τήρηση αρχείων δραστηριοτήτων επεξεργασίας για όλα τα τμήματα της επιχείρησης .Επίσης με την αρχή της λογοδοσίας οι επιχειρήσεις συλλέγουν και επεξεργάζονται προσωπικά δεδομένα και διαμορφώνουν έτσι τις διαδικασίες και τα τεχνικά του συστήματα με τέτοιο τρόπο ώστε να συμμορφώνονται στο κανονισμό .Εν συνεχεία ο κανονισμός υποχρεώνει να υπάρχει αναλυτική τεκμηρίωση για κάθε σκοπό επεξεργασίας με αποτέλεσμα τον απολυτό έλεγχο των προσωπικών δεδομένων.

Έπειτα ο κανονισμός βοηθάει και στην ψηφιακή τεχνολογία καθώς γίνεται καλύτερη χαρτογράφηση στα δεδομένα αφού χρησιμοποιούνται εξελιγμένα μέσα αποθήκευσης μεγάλου όγκου δεδομένων αλλά και εξελιγμένα συστήματα ελέγχου εισόδου για την πλήρη συμμόρφωση με την νομοθεσία. Επιπροσθέτως ενισχύεται η κρυπτογράφηση στα δεδομένα καθώς σύμφωνα με τον κανονισμό είναι υποχρεωτικό να δίδονται συνθηματικά με την

χρήση ψευδώνυμων αλλά και την αποκάλυψη όσο των δυνατών λιγότερων βασικών πληροφοριών στο ευρύ κοινό.



Βασικές καινοτομίες στην ασφάλεια μέσω GDRP Πηγή: European Genome – Phenome Archive 2021

ΚΕΦΑΛΑΙΟ 4 -ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

4.1 ΕΛΛΗΝΙΚΗ

1. Γεωργακόπουλος Θ. (2016) «Η φοροδιαφυγή στην Ελλάδα- Μια έρευνα» ιστοσελίδα διανεοσις 2016 https://www.dianeosis.org/2016/06/tax_evasion_in_greece/

2. Δημόπουλος Χ. (1989) «Η εγκληματολογική προβληματική των σύγχρονων οικονομικών εγκλημάτων» Εκδόσεις «Σάκκουλας»

3. Ευρωπαϊκή επιτροπή για το περιβάλλον (2014) https://www.europarl.europa.eu/greece/resource/static/files/----------.pdf

4. Ελληνική αστυνομία http://www.astynomia.gr/newsite.php?&lang=

5. Επίσημη εφημερίδα της Ευρωπαϊκής ένωσης 2016

6. Θεματολογικά δελτία για την Ευρωπαϊκή ένωσή (2021) https://eur-lex.europa.eu/

7. Κανελλόπουλος Ν. (2018): « Ο νέος γενικός κανονισμός για την προστασία δεδομένων προσωπικού χαρακτήρα GDPR » Taxheaven https://www.taxheaven.gr/circulars/28194/arora-o-neos-genikos-kanonismos-gia-thn-prostasia-dedomenwn-proswpikoy-xarakthra-gdpr

1. Κουρακάκης Ν. (1982) :« Τα οικονομικά εγκλήματα» Εκδόσεις «Σάκκουλας» 1982

2. Κούλης Ι. Ν. (1970) : « Δημόσια Οικονομική» Εκδόσεις «δεύτερη Αθήνα» 1970

3. Μαρκέτος Π. (2018): Περιοδικό Netweek « Το Βατερλό του GDPR» 2018 https://netweek.gr/to-vaterlo-tou-gdpr/

4. Ν. 4177/13 (ΦΕΚ 173 Α/8-8-2013) : Κανόνες ρύθμισης της αγοράς προϊόντων και της παροχής υπηρεσιών και άλλες διατάξεις. Διαθέσιμο στο: https://www.mindev.gov.gr/wp-content/uploads/2018/04/N.4177.pdf

5. Τσουραμάνης Χ. (1996) : «Οικονομική Παραβατικότητα» Εκδόσεις «Έλλην» 1996

6. Τσουραμάνης Χ. (2005): « Ψηφιακή Εγκληματικότητα» Εκδόσεις «Β.Ν. Κατσαρου» 2005

7. Φλώρου Χ., (2013) «Διπλωματική εργασία Διαχείριση Παραβατικότητας μέσω Τεχνικών ασφάλειας στο διαδίκτυο» Πανεπιστήμιο Πειραιά 2013 https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/8483/Florou_Charalampia.pdf?sequence=1&isAllowed=y,

4.2 ΞΕΝΗ

1. Coadvantage.com (χ.χ.) What Happens If Employers Violate Labor Laws? Διαθέσιμο στο: https://www.coadvantage.com/happens-employers-violate-labor-laws/

2. *Dennis (2021) Britannica https://www.britannica.com/topic/cybercrime/Counterfeiting-and-forgery*

3. Earp B. J., Anton I. A., Aiman- Smith L. Stufflebeam H. W. (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values DOI:10.1109/TEM.2005.844927 https://www.researchgate.net/publication/3076864_Examining_Internet_Privacy_Policies_Within_the_Context_of_User_Privacy_Values

4. Gdpr.eu, (2021) What is GDPR, the EU's new data protection law?

5. Hg.org (2021) Unfair competition law https://www.hg.org/unfair-competition.html

6. IFPI (international federation of the photographic industry) 2012 http://www.ifpi.gr/index.html

7. Lawspot.gr https://www.lawspot.gr/nomikes-plirofories/nomothesia

8. Löytömäki S. (2021) Industrial property rights protect intangible assets Διαθέσιμο στο: https://tem.fi/en/industrial-property-rights

9. No author (2021) Violations of Antitrust Laws Διαθέσιμο στο: https://www.impactlaw.com/criminal-law/white-collar/antitrust

10. Society (2021) Digital Currency The emerging technology of digital currency may affect and change how we see, use, and save money in the years to come.

    https://www.nationalgeographic.org/article/digital-currency/

11. Allot (2021) Cryptocurrency and Cybercrime
    https://www.allot.com/cyberhub/cryprocurrency-and-cybercrime/

12. Επίσημος Ιστό τόπος Δίωξης Ηλεκτρονικού Εγκλήματος. Κρυπτονομίσματα https://cyberalert.gr/kriptonomismata/#

13. Δίωξη Ηλεκτρονικού Εγκλήματος (2021)
    https://www.naftemporiki.gr/story/1743136/die-prosoxi-se-diethni-apati-me-upotithemenes-ependuseis-se-kruptonomismata

14. επίσημος Ιστό τόπος του EC3 της Europol (2022)
    https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

15. Επίσημος Ιστό τόπος της Ε. Ε (2022) europa.eu

16. επίσημος Ιστό τόπος της Interpol (2022)

https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats