

# Ασφάλεια δικτύων 5G:

μια ματιά στο μέλλον  
του διαδικτύου των πάντων

## Α. Εισαγωγή

Στο πρόσφατο ταξίδι του στο εξωτερικό, ο Bob βρήκε επιτέλους την ευκαιρία να χαλαρώσει. Είχε περάσει πολύς καιρός από την τελευταία φορά που πήγε διακοπές με την γυναίκα του την Alice. Όντας επικεφαλής οργανισμού με εργοστάσια και γραμμές παραγωγής σε όλη την Ευρώπη, η καθημερινότητά του εξαντλούνταν στο να συντονίζει τις ενέργειες παρακολούθησης των βιομηχανικών συστημάτων και της απόδοσής τους, προσπαθώντας ταυτόχρονα να διατηρήσει σε υψηλά επίπεδα την ποιότητα των παραγόμενων προϊόντων. Η δε Alice, γενική χειρουργός σε μεγάλο νοσηλευτικό ίδρυμα είχε να διαχειριστεί τους ασθενείς της, προσπαθώντας ταυτόχρονα να διατηρείται ενημερωμένη για τα τε-

κταινόμενα στον τομέα της. Παρόλη τη διαφορετικότητα των δραστηριοτήτων τους, το ζευγάρι έβρισκε ένα κοινό σημείο συζήτησης αργά τα βράδια. Την αυτοματοποίηση και βελτιστοποίηση των χρησιμοποιούμενων μεθόδων, με απώτερο στόχο αφενός την αύξηση της παραγωγικότητάς τους, αφετέρου τη διασφάλιση ότι ανά πάσα στιγμή θα ήταν σε θέση να εξυπηρετήσουν έκτακτα συμβάντα.

Σε αντίθεση με παλαιότερες εξορμήσεις όπου χρειάστηκε να επιστρέψουν εσπευσμένα λόγω δύσκολων περιστατικών, αυτή τη φορά ήταν σίγουροι ότι δε θα χρειάζονταν να φύγουν πολύ μακριά από το θέρετρό τους. Ο Bob δεν λάμβανε απλώς συνεχείς ενημερώσεις για τα βιομηχανικά συστήματα των εργοστασίων, αλλά είχε τη

δυνατότητα να τα ελέγξει απομακρυσμένα, σε πραγματικό χρόνο, σε περίπτωση που παρουσιάζονταν μια έκτακτη ανάγκη. Η δε Alice, ήταν σε θέση να εξυπηρετήσει άμεσα ασθενείς της, μέσω του συστήματος τηλε-ιατρικής που είχε εγκατεστημένο στην ταμπλέτα της. Εάν δε τύγχανε ένα έκτακτο περιστατικό, είχε ήδη συνεννοηθεί με το νοσοκομείο στον τόπο διακοπών της και εφόσον απαιτείτο θα χειρουργούσε από εκεί μέσω απομακρυσμένου χειρισμού του ρομποτικού χειρουργού στο νοσοκομείο της. Ενώ πριν από μερικά χρόνια το εν λόγω παράδειγμα θα αποτελούσε σενάριο επιστημονικής φαντασίας, το διαδίκτυο των πραγμάτων (Internet of Things – IoT), αλλά και ευφυής διασύνδεση με ανθρώπους (Internet of Everything – IoE) επέ-



φερε μια νέα πραγματικότητα σε πλήθος επιχειρηματικών τομέων. Η διασύνδεση φυσικών αντικειμένων και συσκευών με την παράλληλη συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο, αποτέλεσε τη βάση για την 4η βιομηχανική επανάσταση, συχνά αναφερόμενη ως Industry 4.0. Η εν λόγω ευφυής διασύνδεση όμως χρειάστηκε έναν βασικό συνδετικό κρίκο<sup>1</sup> για

να αποδώσει τα μέγιστα οφέλη, ο οποίος και ανάγεται στα κινητά δίκτυα 5ης γενεάς (5th Generation - 5G).

## B. Τι είναι το 5G

Το 5G χρησιμοποιείται ως όρος για να περιγράψει τα ψηφιακά δίκτυα κινητής τηλεφωνίας τα οποία, μεταξύ άλλων, παρέχουν πολύ υψηλές ταχύτητες (από 50 Mbps σε πάνω από Gbps) σε σχέση με τα δίκτυα κινητής προηγούμενων γενεών (3G, 4G, κλπ.), αλλά και χαμηλή καθυστέρηση (latency). Ταυτόχρονα όμως, στον όρο 5G ενσωματώνονται και όλα τα απαιτούμενα πρωτόκολλα επικοινωνίας, εξοπλισμός

απευθείας από τους απαιτούμενους πληροφοριακούς πόρους.



**Δρ. Θεόδωρος Στεργίου**  
Αναπληρωτής Γενικός  
Διευθυντής, Cyber Security  
Services, KPMG



**Θεοδόσης Τζούμας**  
Συνέταιρος,  
Παπακωστόπουλος-  
Γρηγοριάδου και Συνεργάτες  
Δικηγορική εταιρεία (CPA Law),  
ανεξάρτητο μέλος του νομικού  
και φορολογικού δικτύου της  
KPMG

παρόχου κινητής τηλεφωνίας (κεραίες, δίκτυο, κλπ.), αλλά και οι επιχειρηματικές δυνατότητες που παρέχουν οι υψηλές ταχύτητες, καθιστώντας το 5G ένα από τα πιο σημαντικά buzzword της εποχής μας.

Το 5G ξεκίνησε από το πρότυπο IMT-2020 του διεθνούς οργανισμού τηλεπικοινωνιών (International Telecommunications Union – ITU), το οποίο έθεσε, από το 2012, τις προδιαγραφές για τα 5G δίκτυα, συσκευές και υπηρεσίες<sup>2</sup>. Εν συνεχεία, ο οργανισμός 3GPP<sup>3</sup>, υπεύθυνος για τον καθορισμό των προτύπων (standards) καθιέρωσε το 5G NR (New Radio) το οποίο κατέθεσε ως απάντηση στο κάλεσμα IMT-2020 της ITU. Αυτή τη στιγμή, τα πρότυπα του 3GPP βρίσκονται στην έκδοση 16 (Release 16<sup>4</sup>), με τον οργανισμό να σχεδιάζει ήδη τις επόμενες δύο εκδόσεις (Release 17<sup>5</sup> και Release 18<sup>6</sup>).

**Βασικά στοιχεία (key drivers) ανάπτυξης του 5G αποτέλεσαν:**

- ▶ Μεγάλη χωρητικότητα δικτύου (capacity).
- ▶ Μεγάλο εύρος ανταλλαγής δεδομένων (bandwidth).

1. Για να είμαστε ακριβείς, η εγκατάσταση πληθώρας συσκευών (π.χ. sensors) και η ολοκληρωτική υιοθέτηση του Internet Protocol 4.0 απαιτεί και τη μετάβαση στην 6η έκδοση του Internet Protocol (IPv6), μιας και η τρέχουσα έκδοση (IPv4) έχει πεπερασμένο αριθμό IP διευθύνσεων που μπορούν να χρησιμοποιηθούν. Με το IPv6, κάθε συσκευή θα μπορέσει να έχει μια μοναδική διεύθυνση ώστε να μπορεί να προσπελαστεί

2. [http://www.itu.int/net/pressoffice/press\\_releases/2015/27.aspx#YA0tRhZS-Mo](http://www.itu.int/net/pressoffice/press_releases/2015/27.aspx#YA0tRhZS-Mo)  
3. <https://www.3gpp.org/about-3gpp/about-3gpp>  
4. <https://www.3gpp.org/release-16>  
5. <https://www.3gpp.org/release-17>  
6. <https://www.3gpp.org/release18>

- ▶ Χαμηλή καθυστέρηση δικτύου (latency).
- ▶ Μεγάλη αξιοπιστία δικτύου (reliability).
- ▶ Αποτελεσματικότητα (efficiency).

Η αξία του 5G αγγίζει, όπως μπορεί να γίνει εύκολα αντιληπτό, όλους τους επιχειρηματικούς τομείς. Η KPMG παρουσίασε το 2019 στο συνέδριο Mobile World Congress, μια παγκόσμια έρευνά της με τίτλο «Unlocking the benefits of 5G for enterprise customers<sup>7</sup>». Βασικά σημεία της έρευνας παρατίθενται παρακάτω:

- ▶ Τα επιχειρηματικά πλάνα για το 5G αφορούν κατά μεγάλη πλειοψηφία συνδιαλλαγές μεταξύ επιχειρήσεων (B2B) έναντι επιχειρήσεων με τελικούς καταναλωτές (B2C), μια διαφορά της τάξης των US\$4.3 τρις.
- ▶ Οι τελικοί καταναλωτές δεν είναι διατεθειμένοι να πληρώσουν το κόστος του νέου δικτύου και υπηρεσιών, κάτι το οποίο είδαμε να συμβαίνει με το 3G και 4G, οπότε και το βάρος θα πέσει στην Βιομηχανία 4.0 και το προαναφερθέν μοντέλο B2B.
- ▶ Τα ανωτέρω σημαίνουν ότι η υιοθέτηση του 5G θα λάβει χώρα πρωτίστως μέσω ιδιωτικών / εμπορικών δικτύων και δευτερευόντως μέσω δημόσιων, όπως δήμους και κοινότητες όπου στόχος είναι η παροχή υπηρεσιών σε τελικούς καταναλωτές.

Ταυτόχρονα, η ανάλυση της KPMG επεσήμανε με τη σειρά της τη σημασία του 5G στην 4η βιομηχανική επανάσταση, με τους τομείς βιομηχανίας και μεταποίησης να ωφελούνται πιο γρήγορα από ότι άλλοι επιχειρηματικοί κλάδοι.

Μέσω των μεγάλων ταχυτήτων του νέου δικτύου και της ευφυούς διασύνδεσης συσκευών, θα παρέχεται η δυνατότητα επεξεργασίας δεδομένων πιο κοντά στη συσκευή (edge computing), με άμεσο όφελος την ανταλλαγή δεδομένων σε πραγματικό χρόνο και την απελευθέρωση του δικτύου από τα μεταφερόμενα δεδομένα.

Δημιουργείται λοιπόν ένα ολόκληρο οικοσύστημα υπηρεσιών, διασύνδεσης, λογισμικού και εξοπλισμού, το οποίο υποστηρίζεται από πληθώρα παρόχων και κατασκευαστών οι οποίοι θα θελήσουν μερίδιο από τα διαφαινόμενα μεγάλα έσοδα.

Στην έκθεση της KPMG, τα προσδοκώμενα παγκόσμια οφέλη σε πέντε διαφορετικούς επιχειρηματικούς τομείς, μέχρι το 2023, είναι πραγματικά ιλιγγιώδη, ακόμα και βάσει των μετριοπαθών προβλέψεών μας:

- ▶ Βιομηχανία: US\$ 206.4 δις
- ▶ Ιατρική: US\$ 45 δις
- ▶ Έξυπνες μετακινήσεις: US\$ 24.3 δις
- ▶ Παρακολούθηση περιβάλλοντος: US\$ 5 δις
- ▶ Gaming: US\$ 236 δις

## Γ. Τι συνεπάγεται αυτό για την ασφάλεια πληροφοριών

Για να γίνει κατανοητό τι συνεπάγεται η ασφάλεια πληροφοριών στα δίκτυα κινητής 5ης γενιάς (5G) θα πρέπει πρωτίστως να αναλυθούν κάποιες ενδεικτικές διαφορές του 5G με το 4G (LTE), οι οποίες συνοψίζονται στους κάτωθι πυλώνες, σύμφωνα με το Thales Group<sup>8</sup>:

- ▶ Χαμηλή υστέρηση δικτύου (latency): η πολύ χαμηλή καθυστέρηση του 5G δικτύου θα διευκολύνει την ανάλυση δεδομένων σε πραγματικό χρόνο, βασικό δομικό συστατικό υπηρεσιών όπως η τηλε-ιατρική, τα αυτοκινούμενα οχήματα, κλπ.
  - ▶ Το δίκτυο 5G έχει τη δυνατότητα να υποστηρίξει έως και 100 φορές περισσότερες διασυνδεδεμένες συσκευές έναντι του δικτύου 4G. Συγκεκριμένα, μέχρι 1 εκατομμύριο συσκευές σε μια γεωγραφική περιοχή ενός τετραγωνικού χιλιομέτρου.
  - ▶ Χαμηλή καταλάνωση, η οποία επιτυγχάνεται λόγω του πυκνού δικτύου (κεραίες, κλπ.) και η οποία θα διασφαλίσει μεγαλύτερο χρόνο ζωής των διασυνδεδεμένων συσκευών.
- Εάν αναλύσουμε λίγο τα ανωτέρω σημεία, τα οποία σε καμία περίπτωση δεν εξαντλούν τις καινοτομίες που εισάγει το 5G, θα δούμε πως αναδεικνύεται πληθώρα προκλήσεων αναφορικά με την ασφάλεια πληροφοριών και προστασία δεδομένων. Ενδεικτικά:
- ▶ Επιχειρηματικοί τομείς όπως η τηλε-ιατρική ή τα αυτοκινούμενα οχήματα απαι-

τούν τη διασφάλιση του οικοσυστήματος που τους υποστηρίζουν. Ένας επιτιθέμενος θα μπορούσε να υποκλέψει τα συστήματα ενός αυτοκινούμενου οχήματος και να προκαλέσει ατύχημα ή να το κλέψει, ενώ μια επίθεση άρνησης υπηρεσιών (DoS – Denial of Service) θα αφαιρούσε από έναν γιατρό, όπως η Alice, τη δυνατότητα να χειρουργήσει απομακρυσμένα έναν ασθενή. Ακόμα χειρότερα, θα μπορούσε να αλλοιώσει τα δεδομένα που ένας βηματοδότης παρέχει σε έναν γιατρό, ο οποίος θα οδηγούνταν σε λάθος διάγνωση για τον ασθενή του, με σοβαρές επιπτώσεις για την υγεία του.

▶ Η πληθώρα διασυνδεδεμένων συσκευών σε τόσο περιορισμένο χώρο, δίνει τη δυνατότητα εκμετάλλευσης τυχόν ευπαθειών, ώστε ένας επιτιθέμενος να τις χρησιμοποιήσει προς ίδιον όφελος, ειδικά εάν οι συσκευές δεν είναι επαρκώς προστατευμένες. Δεν είναι λίγα τα παραδείγματα όπου συσκευές όπως κάμερες παρακολούθησης (CCTV) χρησιμοποιήθηκαν από κακόβουλους χρήστες για την εξαπόλυση επιθέσεων άρνησης υπηρεσίας σε άλλους οργανισμούς<sup>9</sup>.

▶ Η αύξηση του χρόνου ζωής των συσκευών, επιφέρει και την μείωση της ανθρώπινης παρέμβασης αναφορικά με τη συντήρησή τους. Παρόλο που οι συσκευές θα παρακολουθούνται από κάποιο κέντρο, επιθέσεις φυσικής ασφάλειας θα μπορούσαν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση και εκμετάλλευση των συσκευών προς όφελος του επιτιθέμενου. Ταυτόχρονα, η φυσική καταστροφή θα μπορούσε να οδηγήσει σε αδυναμία παροχής υπηρεσιών προς πολίτες. Φανταστείτε έναν δήμο ο οποίος παρέχει έξυπνη σήμανση, φωταγώγηση και διασύνδεση στους πολίτες μέσω μιας συσκευής ανά στύλο. Η καταστροφή της συσκευής θα σήμαινε αφενός τη διακοπή παροχής υπηρεσιών, αφετέρου την κινητοποίηση του μηχανισμού συντή-

7. «Unlocking the benefits of 5G for enterprise customers», KPMG International, 2019.

8. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G>

9. <https://www.csoonline.com/article/3089298/iot-botnet-25-513-cctv-cameras-used-in-crushing-ddos-attacks.html> και <https://www.computerworld.com/article/2996079/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html>

ρσης έναντι άλλων προγραμματισμένων ενεργειών.

► Η χρήση συσκευών σε επίπεδο νοικοκυριού, όπως έξυπνοι μετρητές, έξυπνες συσκευές, κλπ. ενέχει την επεξεργασία προσωπικών δεδομένων. Οι εν λόγω συσκευές θα μπορούσαν να χρησιμοποιηθούν από επιτιθέμενους ώστε να αναγνωρίσουν την ανθρώπινη παρουσία σε ένα οίκημα, με σκοπό να το κλέψουν. Ή ακόμα και την υποκλοπή βίντεο ή/και εικόνων από κάμερες παρακολούθησης προς περαιτέρω εκμετάλλευση (εκβιασμός, κλπ.).

Τα παραπάνω χαρακτηριστικά παραδείγματα, αποτελούν θέματα που οι επαγγελματίες ασφάλειας πληροφοριών / κυβερνοασφάλειας και προστασίας δεδομένων μελετούν εδώ και αρκετό καιρό. Η διαφορά που εισάγει το 5G είναι η πραγμάτωση των επιχειρηματικών σεναρίων και η παροχή των κατάλληλων μηχανισμών για την υλοποίηση όλων όσων εντάσσονται στη σφαίρα της έξυπνης πόλης ή έξυπνης βιομηχανίας.

Τι σημαίνουν λοιπόν τα παραπάνω αναφορικά με την προστασία του 5G οικοσυστήματος; Ενδεικτικά θα μπορούσαμε να αναφέρουμε τα κάτωθι:

► Αναγκαιότητα εγκαθίδρυσης αμοιβαίας εμπιστοσύνης μεταξύ συσκευών και δικτύου: η διασύνδεση πολλών συσκευών μεταξύ τους, χωρίς απαραίτητα να παρεμβάλλεται κάποιο άλλο δίκτυο ή μηχανισμός, απαιτεί τη δημιουργία αμοιβαίας εμπιστοσύνης (mutual trust) μεταξύ των εν λόγω συσκευών και κατ' επέκταση του δικτύου μέσω του οποίου οι εμπλεκόμενοι φορείς θα γίνουν αποδέκτες των ήδη επεξεργασμένων πληροφοριών. Αν λάβουμε υπόψη τον οργανισμό που δουλεύει ο Bob, αυτό θα σήμαινε ότι οι συσκευές που υπάρχουν σε όλο το εργοστάσιο (sensors, κλπ.) είναι μεταξύ τους συνδεδεμένες ανταλλάσσοντας στοιχεία και εντολές σε πραγματικό χρόνο με σκοπό τη διασφάλιση της εφοδιαστικής αλυσίδας και της παραγωγής του προϊόντος βάσει των ορισθέντων κριτηρίων ποιότητας. Ο Bob λαμβάνει στοιχεία τα οποία οι συσκευές έχουν ήδη επεξεργαστεί και αποστέλλει σε υποδομή υπολογιστικού νέφους (ιδιωτικό ή δημόσιο ή υβριδικό) στο οποίο

έχει συνδεθεί ο Bob με την ταμπλέτα του. Όλο το οικοσύστημα των συσκευών στο εργοστάσιο, το υπολογιστικό νέφος, η ταμπλέτα του Bob και τα δίκτυα που υποστηρίζουν τη μεταξύ τους διασύνδεση, πρέπει να είναι σε θέση να συνδέονται και ανταλλάσσουν πληροφορία χωρίς να ανησυχούν για το εάν κάποιος θα μπορέσει να παρεισχύσει στο οικοσύστημα και εισάγει κακόβουλες συσκευές ή εντολές. Ενδεικτικές τεχνολογίες που δύνανται να χρησιμο-

Είναι σίγουρο ότι βρισκόμαστε σε μία χωρίς επιστροφή πορεία προς έναν online κόσμο όπου τα δίκτυα επικοινωνιών θα είναι πανταχού παρόντα αποτελώντας κυριολεκτικά το λεμφικό σύστημα των σύγχρονων κοινωνιών

ποιηθούν για τέτοιες περιπτώσεις είναι το blockchain, όπου επιτυγχάνεται αφενός η εμπιστοσύνη μεταξύ των συνδιαλλασόμενων μερών, αφετέρου η αρχή της μη αποποίησης (non repudiation).

► Πέραν του ελέγχου αυθεντικότητας των συσκευών του οικοσυστήματος, θα πρέπει να διασφαλιστεί η επικοινωνία τους, μέσω ενσωμάτωσης κρυπτογραφικών επεξεργαστών και πρωτοκόλλων. Η κρυπτογράφηση της επικοινωνίας θα διασφαλίσει την εμπιστευτικότητα των στοιχείων και τη μη αποκάλυψή τους σε κακόβουλους χρήστες.

► Σε επίπεδο συσκευής, θα πρέπει να διασφαλιστεί ο διαχωρισμός μεταξύ των δεδομένων που θα ανταλλάσσουν και των μηνυμάτων ελέγχου (control messages), ώστε να επιτευχθεί η αρχή της πολύ-επίπεδης ασφάλειας (multilayer security architecture). Μέσω της πολύ-επίπεδης ασφάλειας, το οικοσύστημα θα μπορεί να πετύχει έναν ικανοποιητικό βαθμό προστασίας από επιθέσεις, έστω και εάν κάποιος μηχανισμός αποτύχει. Για παράδειγμα, μπορεί ένας επιτιθέμενος να υποκλέψει στοιχεία, αλλά δεν θα μπορεί να προγραμματίσει τη συσκευή να διαγράψει τα αρχεία καταγραφής ή να την κλείσει (shut down). Ή ακόμα να αποτραπεί η

μη εξουσιοδοτημένη πρόσβαση από κακόβουλους χρήστες οι οποίοι θα μπορούσαν να χρησιμοποιήσουν τις συσκευές ώστε να στήσουν ένα botnet και εκκινήσουν DDoS attacks.

► Την προστασία των συσκευών που φέρουν τα φυσικά πρόσωπα (wearables, chips, κλπ.) ώστε να αποτρέπεται η κακόβουλη χρήση τους η οποία θα μπορούσε να έχει αντίκτυπο στην υγεία ενός ατόμου ή/και η διαρροή προσωπικών δεδομένων.

► Τη φυσική προστασία των end nodes, ώστε να αποτρέπεται η καταστροφή ή/και βανδαλισμός τους, που θα μπορούσε να οδηγήσει σε μη διαθεσιμότητα του δικτύου.

► Την προστασία του δικτύου 5G (radio access network – RAN) ώστε να μην είναι εύκολο σε έναν επιτιθέμενο να παρεισχύσει σε ένα δίκτυο κινητής τηλεφωνίας και υποκλέψει επικοινωνίες συσκευών ή φυσικών προσώπων.

#### Δ. Τι συνεπάγεται αυτό από άποψη δικαιωμάτων, ατομικών, κοινωνικών και πολιτικών

Από το 2008 έως σήμερα η ανάπτυξη των δικτύων 4G οδήγησε στην εκρηκτική –με τα μέχρι τότε δεδομένα– ανάπτυξη αυτού που ονομάζουμε κοινωνία της πληροφορίας, δίνοντας στους ανθρώπους τη δυνατότητα να μοιράζονται ιδέες και να επικοινωνούν κυριολεκτικά στα πέρατα του κόσμου. Αυτό αποτελούσε επίσης και μία εγγενή συνθήκη εκδημοκρατισμού για κοινωνίες που είχαν μείνει απομονωμένες και υστερούσαν έναντι του σύγχρονου δυτικού κόσμου (βλ. το παράδειγμα της αφρικανικής ηπείρου). Η απελευθέρωση της πληροφορίας και η πρόσβαση σε αυτή από όλους, είτε ως καταναλωτές της πληροφορίας, είτε ως δημιουργούς αυτής, αποτελεί το πιο «βίαιο» φαινόμενο εκδημοκρατισμού στην ιστορία. Ένα φαινόμενο ωστόσο που έχει σαφώς δύο όψεις. Η αρνητική όψη έχει να κάνει ακριβώς με τον έλεγχο της πληροφορίας ή της δυνατότητας χειραγώγησης αυτής<sup>10</sup>. Πολύ εύστοχα αναφέ-

10. Βλ. ενδεικτικά τη συζήτηση γύρω από την αναστολή υπηρεσίας από το Twitter προς τον πρόεδρο Trump. Ανεξάρτητα αν η συμπεριφορά του τελευταίου παραβιάζει ευθέως τους



ρεται ότι η πληροφορία είναι το πετρέλαιο του 21ου αιώνα και μάλιστα η ροή της μπορεί να ελεγχθεί. Είναι σαφές λοιπόν ότι η ακρίβεια, η πληρότητα, η ακεραιότητα και η αυθεντικότητα της πληροφορίας είναι θεμελιώδες ζήτημα, καταρχάς ασφάλειας των πληροφορικών συστημάτων, αλλά κυρίως πρόκειται για ένα διακύβευμα δημοκρατίας. Στο πλαίσιο αυτό, ανεξάρτητα από το αν πιστεύει κανείς ότι το 5G συνδυασμένο με το edge computing είναι πράγματι μια τεχνολογική επανάσταση ή όχι, αυτό που είναι σίγουρο είναι ότι βρισκόμαστε σε μία χωρίς επιστροφή πορεία προς έναν online κόσμο όπου τα δίκτυα επικοινωνιών θα είναι πανταχού παρόντα αποτελώντας κυριολεκτικά το λεμφικό σύστημα των σύγχρονων κοινωνιών.

Και το πιο σημαντικό είναι ότι σε αυτή τη νέα εποχή την πληροφορία θα την παράγουν πρωτίτως, όχι οι άνθρωποι, αλλά ένα οικοσύστημα αναρίθμητων διασυνδεδεμένων συσκευών που θα αλληλοεπιδρούν με τους ανθρώπους. Η πραγματικότητα είναι

ότι τα μηχανήματα αρχίζουν να αναλαμβάνουν ένα ολοένα και μεγαλύτερο μέρος του ανθρώπινου «γνωστικού φορτίου», επιτρέποντάς μας να επαναπροσδιορίσουμε το δικό μας γίνεσθαι πάνω σε άλλα -ελπίζουμε πιο πολύτιμα- ζητήματα. Ήδη σήμερα υπάρχουν περισσότερες από 20 δισεκατομμύρια διασυνδεδεμένες συσκευές και ο αριθμός τους αναμένεται να ανέλθει σε περισσότερες από 75 δισεκατομμύρια μόλις το 2025, ακολουθώντας μία εκθετική άνοδο. Αλήθεια φοράτε smart watch ή έχετε απομακρυσμένη πρόσβαση μέσα από το κινητό σας στο συναγερμό και τις κάμερες του σπιτιού σας, τα οποία σας στέλνουν push notifications; Ε, αυτό είναι μόνον η αρχή. Πράγματι, ιδίως τα σύγχρονα δικτυωμένα σπίτια μπορούν να μας δώσουν μία πρώτη ιδέα για την καθολική διάσταση που θα λάβει τα αμέσως επόμενα χρόνια η κοινωνία της πληροφορίας και σε αυτό το 5G δεν είναι τίποτα παραπάνω από μία παράμετρος, ένας τεχνολογικός επιταχυντής των εξελίξεων, αλλά παράλληλα και ένα αναπόδραστο ευαίσθητο σημείο, ένα single point of failure. Δεν χρειάζεται να είναι κανείς ειδήμων περί την ασφάλεια των επικοινωνιών για να αντιληφθεί σαφώς τις ευκαιρίες, αλλά εν προκειμένω και τους κινδύνους αυτού του οικοσυστήματος. Αναπόδραστα στο μέλλον θα οριοθετούμε την ιστορική εξέλιξη της κοινωνίας της πληροφορίας ως την εποχή πριν και μετά το 5G.

Σε αυτό το οικοσύστημα που είναι ήδη εδώ, υπάρχουν μία σειρά από προκλήσεις,

ηθικές και νομικές, με πρώτη και κύρια το αναπόδραστο του πράγματος. Ο νέος γενναίος online κόσμος δεν είναι μία πραγματικότητα που κανείς μπορεί να επιλέξει αν θα συμμετάσχει ή όχι. Αυτή η επιλογή απλά δεν υφίσταται<sup>11</sup>. Επίσης η πολλαπλότητα των διασυνδεδεμένων συσκευών, πολύ συχνά εικονικών συσκευών και εφαρμογών και η πληθώρα των παραμέτρων επεξεργασίας καθιστά πρακτικά αδύνατο για το υποκείμενο τον έλεγχο των επεξεργασιών που τον αφορούν. Ομοίως πλέον ομιλούμε για ένα οικοσύστημα με παγκόσμια διάσταση, που έχει ήδη κατά πολύ καταλάβει υπερεθνικές διαστάσεις. Στο πλαίσιο αυτό, τα υφιστάμενα επιχειρηματικά μοντέλα είναι καταδικασμένα να αλλάξουν, γεγονός που θα επιβάλει αλλαγές σε βασικές ρυθμιστικές και νομικές παραδοχές, καθώς ο νομικός μας πολιτισμός δομήθηκε για να περιγράψει και να υπηρετήσει ένα μοντέλο λειτουργίας μίας κοινωνίας που τώρα αλλάζει και αλλάζει ταχύτατα και δραματικά. Και τέλος, η διάδραση των ανθρώπων και των διασυνδεδεμένων συσκευών αναπόδραστα δημιουργεί νομικά και ηθικά παράδοξα.

Για παράδειγμα πώς θα οριοθετούμε πλέον τον ιδιωτικό και το δημόσιο χώρο; Όλοι ομιλούμε και υπερασπιζόμαστε το δικαίωμα

όρους χρήσης της υπηρεσίας γύρω από τη «λεκτική μίσους» [https://blog.twitter.com/en\\_us/topics/company/2020/suspension.html](https://blog.twitter.com/en_us/topics/company/2020/suspension.html), η πράξη αυτή αποτελεί ένα πρώτο ιστορικό προηγούμενο που θέτει σαφώς θέματα δημοκρατίας και περιορισμού του δημόσιου λόγου από έναν digital gatekeeper που δεν παύει να είναι μία ιδιωτική εμπορική επιχείρηση. Το θέμα αυτό το έχει πολύ εύστοχα και με επάρκεια σχολιάσει ο ίδιος ο Δ/νων Σύμβουλος & ιδρυτής του Twitter, Jack Dorsey <https://twitter.com/jack/status/1349510771928010753>.

11. Θυμίζει εν πολλοίς την απόπειρα νομάδων της σύγχρονης εποχής να ζήσουν εκτός grid, ήτοι χωρίς να είναι διασυνδεδεμένοι στα δίκτυα διανομής ηλεκτρικής ενέργειας.



στην ιδιωτικότητα, αλλά όλοι μας αυξάνουμε δραματικά την πληροφορία της ιδιωτικής μας σφαίρας που καθιστούμε ηθελήμενα ορατή στο διαδίκτυο (privacy paradox). Εν είδει μεταφοράς, είναι πρακτικά σαν να αναζητούμε μετ' επιτάσεως μία κάποια ιδιωτικότητα, αλλά παράλληλα να ανοίγουμε διάπλατα τις κουρτίνες του σπιτιού μας και μάλιστα να προσκαλούμε να μας παρατηρήσουν στην ιδιωτική μας σφαίρα.

Ομοίως, απλά και μόνον η βασική παραδοχή περί δήλωσης βουλήσεως ως θεμελιώδης αρχή του δικαίου μας, τίθεται εν αμφιβολώ. Δήλωση βουλήσεως ποιανού, του ανθρώπινου παράγοντα ή της συσκευής/εφαρμογής; Στη βιβλιογραφία η διαδικασία αυτή περιγράφεται ως βελτιστοποίηση (sic) της διαδικασίας λήψης απόφασης με τη χρήση τεχνητής νοημοσύνης ("AI enabled improvement of human decision making by IoT applications"), ωστόσο αυτό είναι ένας εύσχημος επιστημονικός όρος να περιγράψει κανείς ότι την αποφασιστική εξουσία και την επιλογή δεν την έχει πλέον το υποκείμενο ή δεν την έχει πρωτογενώς το υποκείμενο, αλλά αντιθέτως ότι η απόφαση, είτε λαμβάνεται από τη μηχανή/εφαρμογή, είτε μοχλεύεται προς το υποκείμενο από την τελευταία<sup>12</sup>.

Και μέσα σε όλον αυτό τον προβληματισμό προκύπτουν και ακόμα πιο θεμελιώδη ζη-

τήματα δημοκρατίας, αναφορικά με τη διακυβέρνηση της πληροφορίας, τους digital gatekeepers κάθε είδους<sup>13</sup>, την ασφάλεια και τη διαθεσιμότητα των δικτύων.

Στο πλαίσιο αυτό η ασφάλεια των δικτύων 5G τίθεται ως ζήτημα κορυφαίας σημασίας, καθώς αυτά καθίστανται η απαραίτητα κρίσιμη υποδομή που θα υποστηρίξει τη συνδεσιμότητα και διαλειτουργικότητα αυτού του νέου κόσμου. Παράλληλα δε με την ασφάλεια αναδύεται και το ζήτημα της ιδιωτικότητας και του δικαιώματος των ατόμων να ελέγχουν ποιες πληροφορίες σχετίζονται με αυτούς και κατά πόσον μπορούν να συλλεχθούν, να αποθηκευτούν και από ποιον.

### Ε. Οι μέχρι στιγμής προσεγγίσεις για τη διασφάλιση της ασφάλειας

Το 5G πέραν των τεχνολογικών δυνατοτήτων του, συνεπάγεται σε τεχνικό επίπεδο έναν ουσιώδη μετασχηματισμό της αρχιτεκτονικής των δικτύων με μεγαλύτερη έμφαση στο λογισμικό και λιγότερο στο υλισμικό (infrastructures). Στη βάση αυτή όλες οι μελλοντικές αναβαθμίσεις του και επόμενες γενεές θα είναι κατά βάση ενημερώσεις λογισμικού όπως οι τρέχουσες αναβαθμίσεις που κάνουμε στο

smartphone μας και σε κάθε περίπτωση η βαρύτητα της μετεξέλιξης θα αφορά το λογισμικό. Ως εκ τούτου, λόγω των προφανών θεμάτων κυβερνοασφάλειας, το πιο δύσκολο μέρος διασφάλισης της ακεραιότητας των δικτύων 5G είναι να επανεξετάσουμε τον τρόπο με τον οποίο το διασφαλίζουμε αυτό, τόσο για το δίκτυο καθαυτό, όσο και για το οικοσύστημα συσκευών και εφαρμογών που θα συμβιώσουν και θα αλληλοεπιδρούν με αυτό.

Προσπαθώντας να δώσουν απαντήσεις σε αυτά τα ερωτήματα τα σχετιζόμενα με την ασφάλεια των δικτύων 5G, τόσο η αμερικανική κυβέρνηση, όσο και η Ευρωπαϊκή Επιτροπή έχουν αναλάβει πρωτοβουλίες, εν πολλοίς με κοινό ζητούμενο, αλλά με διαφορετική προσέγγιση.

#### i. US Clean Network Program

Η αμερικανική πρωτοβουλία που ανακοινώθηκε εντός του θέρους του 2020 ακολουθεί το επιτυχημένο προηγούμενο της CALEA Act<sup>14</sup> της δεκαετίας του '90 η οποία απαιτήθηκε κατά τη μετάβαση από τα αναλογικά στα ψηφιακά δίκτυα και στοχεύει στο να ελέγξει την προσφορά και κατ' επέκταση αξιοποίηση του τεχνολογικού εξοπλισμού στο δυτικό κόσμο από αγνωρισμένους και προς τούτο πιστοποιημένους τεχνολογικούς παρόχους. Αν και έχει ασκηθεί κριτική ότι αυτή η προσέγγιση

12. Βλ. το παράδειγμα των αυτο-οδηγούμενων (self-driving) αυτοκινήτων και την τυχόν ευθύνη σε περίπτωση πρόκλησης ατυχήματος.

13. Βλ. ενδεικτικά τη ρυθμιστική απόπειρα της ΕΕ με την έκδοση σχεδίων Οδηγιών για τις ψηφιακές πλατφόρμες [https://ec.europa.eu/commission/presscorner/detail/el/ip\\_20\\_2347](https://ec.europa.eu/commission/presscorner/detail/el/ip_20_2347).

14. Communication Assistance for Law Enforcement Act.

γηση δεν δίνει απάντηση στον πυρήνα του ζητήματος ασφάλειας που πράγματι είναι υπαρκτός και ότι αποτελεί μία ακόμα διάσταση του εμπορικού πολέμου της δύσης με την Κίνα, αποτελεί ομολογουμένως ένα συνεπές και ευρύ φάσμα μέτρων, καθώς δεν καλύπτει μόνον τον δικτυακό εξοπλισμό, αλλά επεκτείνεται και στις υπηρεσίες, είτε πρόκειται για υπηρεσίες προς παρόχους τηλεπικοινωνιών (carrier services), είτε προς καταναλωτές (store services & apps), αφορά δηλαδή το σύνολο του οικοσυστήματος που ονομάζουμε υπηρεσίες ηλεκτρονικών επικοινωνιών.

## ii. EU toolbox

Η Ευρωπαϊκή Επιτροπή ακολούθησε μία διαφορετική προσέγγιση προκρίνοντας το λειτουργικό κριτήριο και την εφαρμογή μίας «εργαλειοθήκης», ήτοι μίας σειράς κριτηρίων που θα πρέπει να πληρούν τα δίκτυα και κατ' επέκταση ο δικτυακός εξοπλισμός των 5G δικτύων με στόχο τον μετριασμό των κυριότερων κινδύνων κυβερνοασφάλειας. Ο απώτερος στόχος είναι η δημιουργία ενός ισχυρού και αντικειμενικού πλαισίου μέτρων ασφαλείας για τα δίκτυα 5G σε ολόκληρη την ΕΕ, μέσω συντονισμένων προσεγγίσεων μεταξύ των κρατών μελών. Και εδώ ωστόσο είναι παρόν το υποκειμενικό κριτήριο, ήτοι η αξιολόγηση του προφίλ ασφάλειας των προμηθευτών δικτυακού εξοπλισμού και η πολλαπλότητα των πηγών προμήθειας, αποτρέποντας τη δημιουργία σχέσεων εξάρτησης και κατ' επέκταση εγγενείς σχεδιαστικές αδυναμίες στα δίκτυα, πολλώ δε μάλλον έναντι προμηθευτών για τους οποίους είναι δυνατό μελλοντικά να τεθούν ζητήματα ασφάλειας και ακεραιότητας.

## ΣΤ. Οδεύουμε προς μία νέα ρυθμιστική προσέγγιση;

Ζούμε πλέον σε έναν online κόσμο και αυτός ο μετασχηματισμός θα επιταχύνεται όλο και περισσότερο. Στο πλαίσιο αυτό, το «Κουτί της Πανδώρας», υπό την έννοια των κινδύνων, αλλά και των αλλαγών και ευκαιριών, είναι ανοιχτό και αυτό δεν είναι απαραίτητα κακό ακριβώς γιατί η ιστορική αλλαγή που μόλις έχουμε αρχίσει να βιώνουμε, κρύβει μία διάσταση τεχνολογικής προόδου, σε έκταση και ένταση που

## ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΗΝ KPMG

Η KPMG είναι ένας παγκόσμιος οργανισμός ανεξάρτητων εταιρειών παροχής Ελεγκτικών, Φορολογικών και Συμβουλευτικών υπηρεσιών. Δραστηριοποιούμαστε σε 146 χώρες και περιοχές και για το οικονομικό έτος 2020 απασχολήσαμε περίπου 227 000 άτομα, σε εταιρείες-μέλη παγκοσμίως. Κάθε εταιρεία της KPMG είναι νομικά διακριτή και αυτοτελής οντότητα και αυτοχαρακτηρίζεται ως τέτοια. Η KPMG International Limited είναι ιδιωτική Αγγλική εταιρεία περιορισμένης ευθύνης με εγγυητικές εισφορές. Η KPMG International Limited και οι σχετικές εταιρείες με αυτή δεν παρέχουν υπηρεσίες σε πελάτες.

## ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΗΝ Παπακωστόπουλος-Γρηγοριάδου & Συνεργάτες

Η Παπακωστόπουλος-Γρηγοριάδου και Συνεργάτες, Δικηγορική Εταιρεία είναι ανεξάρτητη εταιρεία, μέλος του διεθνούς δικτύου νομικών και φορολογικών υπηρεσιών της KPMG, διαθέτει εξειδικευμένους δικηγόρους και παρέχει αποτελεσματική νομική υποστήριξη και προστασία στους πελάτες της.

Οι υπηρεσίες που παρέχει περιλαμβάνουν τη δικαστηριακή εκπροσώπηση, τη διαπραγμάτευση συναλλαγών, καθώς και ένα ευρύ φάσμα νομικών συμβουλών στους τομείς της φορολογίας, του δημοσίου τομέα, των εταιριών, συμπεριλαμβανομένων των μετασχηματισμών και της αναδιάρθρωσης επιχειρήσεων, του εργατικού και κοινωνικοασφαλιστικού δικαίου, του οικονομικού δικαίου και της Κεφαλαιαγοράς, του Ανταγωνισμού, των Κρατικών Ενισχύσεων καθώς και της οικονομικής εγκληματικότητας.

ουδέποτε έχει βιώσει η ανθρωπότητα στο παρελθόν. Αυτό είναι προφανές ακόμα και στην παρούσα πανδημική περίοδο, όπου βιώνουμε αλλαγές -με τεχνολογικό υπόβαθρο- σε συμπεκνωμένο χρόνο. Αλλαγές που παλαιότερα θα χρειαζόνταν δεκαετίες για να ολοκληρωθούν, τώρα υλοποιούνται σε ορίζοντα ετών ή ακόμα και μηνών. Η μεγάλη εικόνα συνηγορεί στο ότι διάγουμε μία εποχή όπου βιώνουμε δύο τεχνολογικές επαναστάσεις ταυτόχρονα.

Εν προκειμένω, το 5G -όπως ήδη ειπώθηκε- δεν φέρνει από μόνο του την επανάσταση στην κοινωνία της πληροφορίας, είναι ωστόσο η απαραίτητη τεχνολογική προϋπόθεση, το υπόβαθρο συνδεσιμότητας, πάνω στο οποίο θα δομηθεί όλο το νέο τεχνολογικό οικοσύστημα. Το οικοσύστημα αυτό είναι ένας νέος online κόσμος, με αμέτρητες δυνατότητες και ευκαιρίες, ένα οικοσύστημα που θα μεταλλάξει το γίνεσθαι και το επιχειρείν όπως το γνωρίζουμε σήμερα. Το γεγονός αυτό θέτει αναπόδραστα στα όριά του όλο το ρυθμιστικό και νομικό πλαίσιο, συμπεριλαμβανομένου του δικαίου των προσωπικών δεδομένων και όχι μόνο. Ωστόσο το 5G δεν αντιδιαστέλεται την ιδιωτικότητα, είναι λάθος να το πιστεύουμε αυτό. Το ρυθμιστικό πλαίσιο σήμερα εδράζεται επί συγκεκριμένων πα-

ραδοχών που αύριο πλέον δεν θα ισχύουν ή ίσως ακόμη και σήμερα σε κάποιες περιπτώσεις να έχουν καταστεί κενές περιεχομένου. Επομένως χρειάζεται όλα αυτά τα ζητήματα να τα αξιολογήσουμε και να διαμορφώσουμε ένα νέο πλαίσιο, ένα «έξυπνο» και όχι στατικό πλαίσιο με πυρήνα την έννοια της «λογοδοσίας».

Σε ένα νέο κόσμο όπου πλέον η ιδιωτικότητα και η οριοθέτηση του δημόσιου και ιδιωτικού έχει λάβει μία νέα διάσταση, όπου πλέον ομιλούμε για μία νέα μορφή ιδιωτικότητας (ιδιωτικότητα 4.0), είναι θεμελιώδες και προαπαιτούμενο στην εξίσωση του τεχνολογικού μετασχηματισμού που διάγουμε, ο κίνδυνος της ασφάλειας, είτε λαμβάνει τη μορφή της παραβίασης, είτε τη μορφή της διακινδύνευσης της αδιάλειπτης διαλειτουργικότητας, να έχει επαρκώς αντιμετωπιστεί προκειμένου να επιτύχουμε το μετριασμό των κινδύνων και την αναγκαία τεχνολογική ουδετερότητα. Ακριβώς για αυτό το λόγο είναι τόσο σημαντική αυτή η συζήτηση, καθώς η εξασφάλιση του διακυβεύματος της ασφάλειας των δικτύων είναι πρωτόλειο ζήτημα πριν περάσουμε στα ακόμα πιο δύσκολα νομικά και κυρίως ηθικά ζητήματα που θέτει η επανάσταση στην κοινωνία της πληροφορίας που το 5G και το edge computing κομίζουν. 