



# ΠΛΗΡΟΦΟΡΟΛΟΓΙΚΟΣ ΦΟΡΕΥΜΑ

Περιοδική έκδοση της Ένωσης Πληροφορικών Ελλάδας

Τεύχος 19ο

Δεκέμβριος 2022

Διανέμεται ελεύθερα





Περιοδική έκδοση της  
Ένωσης Πληροφορικών Ελλάδας  
[www.epe.org.gr](http://www.epe.org.gr)

### Τεύχος 19<sup>ο</sup> – Δεκέμβριος 2022

Διανέμεται ελεύθερα

Επικοινωνία:

[newsletter@epe.org.gr](mailto:newsletter@epe.org.gr)

#### Συντακτική ομάδα:

- Φώτης Αλεξάκος
- Νίκος Αναστόπουλος
- Χάρης Γεωργίου
- Νεκτάριος Μουμουτζής
- Γιάννης Φαρσάρης

Οι απόψεις των συντακτών είναι  
προσωπικές και δεν εκφράζουν  
απαραίτητα την ΕΠΕ



Το περιεχόμενο του Πληροφορικού  
διανέμεται υπό άδεια [Creative Commons  
BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/) (Αναφορά πηγής - Μη εμπορι  
κή χρήση - Παρόμοια διανομή)

Εικόνα εξωφύλλου: [TimSon Foox](https://www.timsonfoox.com/)

Το λογότυπο του Πληροφορικού είναι μια  
ευγενική προσφορά του γραφίστα  
[Λευτέρη Παναγουλόπουλου](https://www.lefteri.panagoulou.com/)

## ΠΕΡΙΕΧΟΜΕΝΑ

✓ **Σύσταση σε σώμα** των νέων  
οργάνων της ΕΠΕ

✓ Ένα πολύ σημαντικό  
προνόμιο, προσβάσιμο σε  
όλους μας

// Δημήτρης Τσίγκος

✓ **Συνέντευξη με τον κ. Διομήδη  
Σπινέλλη**, Καθηγητή Τεχνολογίας  
Λογισμικού στο Οικονομικό  
Πανεπιστήμιο Αθηνών

✓ **Peopleware**

// Νεκτάριος Μουμουτζής

✓ **Φόρεσε το άσπρο καπέλο  
του χάκερ**

// Γιάννης Φαρσάρης

✓ **Απομακρυσμένη Ηλεκτρονική  
Ψηφοφορία**

// Χάρης Β. Γεωργίου

✓ **Brain – train / Γρίφοι &  
προβλήματα από την Επιστήμη  
των Υπολογιστών για μαθητές**

// Φώτης Αλεξάκος

## ✓ Σύσταση σε σώμα των νέων οργάνων της Ένωσης Πληροφορικών Ελλάδας

Την Κυριακή 27/11/2022 ολοκληρώθηκαν οι αρχαιρεσίες και ανακοινώθηκε το πρακτικό της Κεντρικής Εφορευτικής Επιτροπής για τις εκλογές των κεντρικών οργάνων της ΕΠΕ, οι οποίες διεξήχθησαν ηλεκτρονικά στις 25-27/22/2022, ομαλώς και σύμφωνα με τις προβλέψεις του Καταστατικού.

Στις αντίστοιχες συνεδριάσεις που διεξήχθησαν αμέσως μετά, τα νέα Όργανα της ΕΠΕ συστάθηκαν σε σώμα με τις παρακάτω συνθέσεις:

### Διοικητικό Συμβούλιο:

- Πρόεδρος: **Σιδηρόπουλος Αντώνιος**
- Αντιπρόεδρος: **Κιομουρτζής Ιωάννης**
- Γενικός Γραμματέας: **Γεωργίου Χαρίλαος**
- Ειδικός Γραμματέας: **Αλεξάκος Φώτης**
- Ταμίας: **Φάκας Ιωάννης**

### Επιτροπή Δεοντολογίας:

- Πρόεδρος: **Μουμουτζής Νεκτάριος**
- Αντιπρόεδρος: **Χριστόπουλος Δημήτριος**
- Γραμματέας: **Φαρσάρης Ιωάννης**

### Ελεγκτική Επιτροπή:

- Πρόεδρος: **Σερβετάς Αλέξανδρος**
- Αντιπρόεδρος: **Τσιάμη Χριστοφίλη**
- Γραμματέας: **Συριτζίδου Ελένη**

Τέλος, μετά από ομόφωνη απόφαση του νέου ΔΣ για σχετική πρόταση, έγινε αποδεκτή η πρόσκληση πλήρωσης της θέσης του Γενικού Διευθυντή (βλ. Εσωτ. Κανονισμός, άρθρο 5) από τον πρώτο επιλαχόντα για το ΔΣ:

### Γενικός Διευθυντής: **Αναστόπουλος Νίκος**

Σύμφωνα με το Καταστατικό της ΕΠΕ, η θητεία των νέων κεντρικών οργάνων έχει **διάρκεια 30 μήνες**. Ευχόμαστε καλή θητεία και καλή επιτυχία σε όλες-όλους.

Το Διοικητικό Συμβούλιο  
της Ένωσης Πληροφορικών Ελλάδας

URL: <https://www.epe.org.gr>, <mailto:info@epe.org.gr>

Ένωση Πληροφορικών Ελλάδας





## ✓ Ένα πολύ σημαντικό προνόμιο, προσβάσιμο σε όλους μας!

// Γράφει ο **Δημήτρης Τσίγκος**



*Photo by [Shahadat Rahman](#)*

Η **Ένωση Πληροφορικών Ελλάδας** δεν είναι μια συνηθισμένη περίπτωση επαγγελματικού & επιστημονικού σωματείου. Πέραν πάσης αμφιβολίας, είναι ένας οργανισμός που χαρακτηρίζεται από όραμα, ποιότητα και ανιδιοτέλεια. Χαρακτηριστικά που πλέον σπανίζουν όχι μόνο στον χώρο των σωματείων αλλά και γενικά στην κοινωνία μας.

Σήμερα η ελίτ που κρατά τις τύχες της χώρας αρχίζει να ψελλίζει για την πληροφορική παιδεία, μάλιστα (ακόμα) με έναν, ας μου επιτραπεί, 'φολκορικό' και 'επαρχιωτικό' τρόπο (μιλούν βλέπετε για 'εκπαίδευση στην τεχνητή νοημοσύνη' και άλλα τέτοια χαριτωμένα).

Στα τέλη της δεκαετίας του 1990, αρχικά σαν προπτυχιακός φοιτητής, συμμετείχα στους

αγώνες ώστε οι πτυχιούχοι πληροφορικής να ...έχουν το δικαίωμα να διοριστούν ως καθηγητές πληροφορικής. Μέχρι τότε, την ανάγκη την κάλυπταν γυμναστές και θεολόγοι με σεμινάρια 400 ωρών. Αυτή ήταν η αντίληψη του ελληνικού κράτους για την επιστήμη των υπολογιστών.

Στη συνέχεια, αν δεν κάνω λάθος από το 2003, προωθούμε την πρόταση για το ΕΘΕΠΕ, το επιμελητήριο πληροφορικής ως μια ανεξάρτητη δημόσια αρχή που θα συμβουλευεί το κράτος για τα ζητήματα της πληροφορικής. Ακόμα μια φορά ήμασταν μπροστά από την εποχή μας - αργά η γρήγορα το ΕΘΕΠΕ θα γίνει πραγματικότητα. Αναρωπιέται βέβαια κανείς γιατί 'στις δυο πλατείες' (σύνταγμα και κολωνάκι) έπρεπε να περιμένουν είκοσι χρόνια... τόσα ξέρουν, τόσα κάνουν. Αυτή είναι η απάντηση που δίνω προσωπικά μετά την απογοήτευση τόσων ετών, αυτό όμως δεν αναιρεί την τεράστια αξία της συνεισφοράς της Ένωσής μας όλα αυτά τα χρόνια.

Υπάρχει και πλήθος άλλων πρωτοβουλιών αιχμής, από την ψηφιακή στρατηγική το 2007 έως την αξιολόγηση των προγραμμάτων σπουδών των ελληνικών πανεπιστημίων (ως προς την ονομαστική πληρότητά τους) και πολλές ακόμα. Όλες χαρακτηρίζονται από μακρόπνοο όραμα και υψηλή ποιότητα ενώ είναι αποτελέσματα εθελοντικής, ανιδιοτελούς προσπάθειας των μελών μας. Η περίπτωση της Ένωσης Πληροφορικών Ελλάδας είναι πραγματικά μοναδική, για τα ελληνικά και όχι

μόνο δεδομένα. Έχει γίνει μια τεράστια προσπάθεια που ήδη έχει φέρει αξιόλογα αποτελέσματα.

Τώρα μένει να αγκαλιαστεί μαζικά από τους νέους συναδέλφους ώστε να μπορέσει να απαντήσει στα ζητήματα του σήμερα και του αύριο στην πληροφορική. Ζητήματα επαγγελματικά, ερευνητικά, ακαδημαϊκά αλλά και κοινωνικά, αφού η ψηφιακή ελευθερία πλέον ταυτίζεται με την ευρύτερη ελευθερία.

Για να γίνει αυτό, πρέπει όλοι μας να κάνουμε ένα μικρό βήμα: Να συνειδητοποιήσουμε πως είναι ένα μεγάλο προνόμιο το να συμμετέχει κανείς σε μια τέτοια ένωση και να αναλάβουμε δράση με τρόπο αντάξιο του προνομίου αυτού.

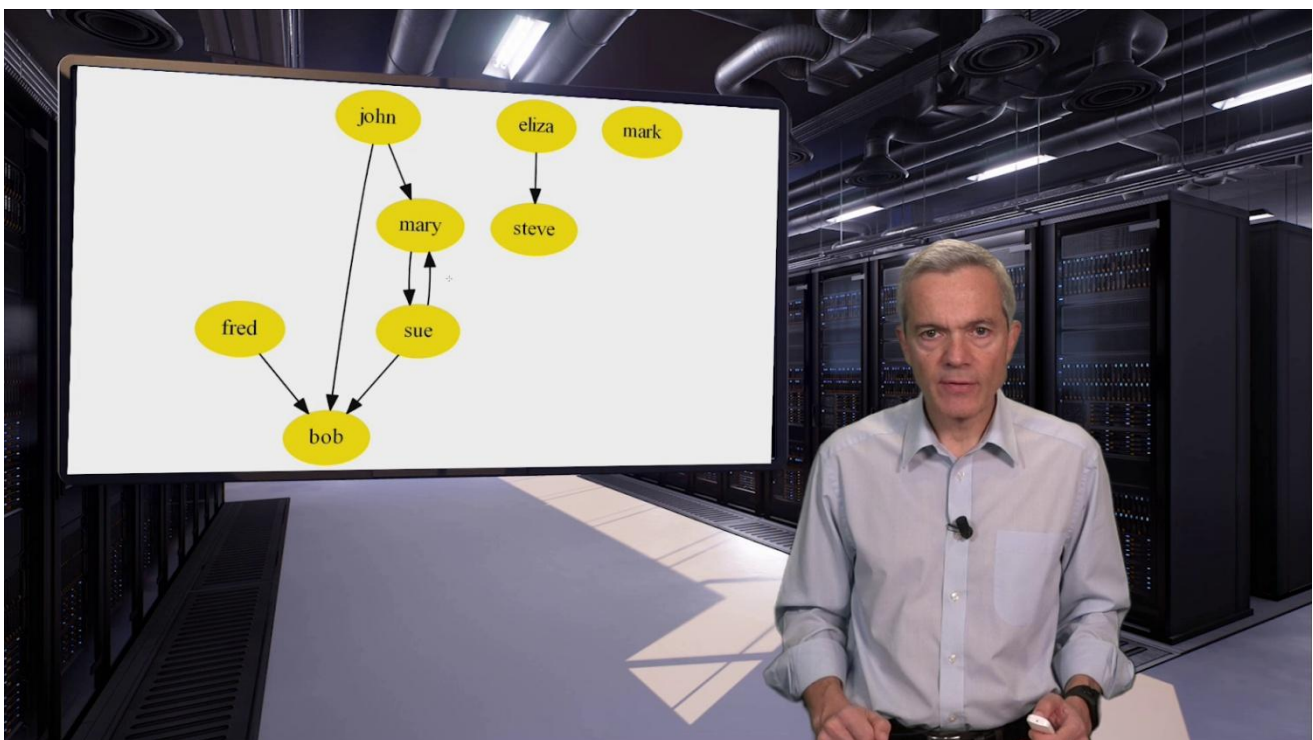
Όταν ήμουν προπτυχιακός άκουγα ότι η επιστήμη μας θα καθορίσει τον 21ο αιώνα. Αφού έχουμε διαβεί ήδη το 20% του αιώνα, η αλήθεια αυτής της θέσης είναι πασιδήλη. Μένει σε όλους εμάς, τους ανθρώπους που θεραπεύουμε την πληροφορική σε όλες της τις πτυχές να ασκήσουμε τα δικαιώματα που απορρέουν από το μεγάλο αυτό προνόμιο.

Η κοινωνία το περιμένει από εμάς. Να ανταποκριθούμε. Ας ξεκινήσουμε με το απλούστερο όλων: Συμμετοχή στις διαδικασίες.

Η πληροφορική ορίζει πλέον τη δημόσια σφαίρα και αυτή με τη σειρά της καθορίζει την κοινωνία που ζούμε. Το τι θα συμβεί, εξαρτάται σε τελική ανάλυση από την δράση καθενός και καθεμιάς από εμάς.

## ✓ Συνέντευξη με τον κ. Διομήδη Σπινέλλη

Καθηγητή Τεχνολογίας Λογισμικού  
στο Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας  
του Οικονομικού Πανεπιστημίου Αθηνών



Διάλεξη στο μαζικό ανοιχτό διαδικτυακό μάθημα (MOOC) της πλατφόρμας edX με τίτλο [«Unix Tools Data, Software and Production Engineering» \(2020\)](#)

Σπουδάσατε για χρόνια στη Μεγάλη Βρετανία, όμως επιστρέψατε στην Ελλάδα για να προσφέρετε τις υπηρεσίες σας στο Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Οικονομικού Πανεπιστημίου Αθηνών. Ποιο ήταν το κίνητρο που σας ώθησε να γυρίσετε στη χώρα μας και δεν επιλέξατε μια καριέρα στο εξωτερικό;

Με κρατάει στην Ελλάδα η αγάπη μου για τη χώρα μας. Όταν ταξιδεύω στο εξωτερικό πάντα χαίρομαι όταν επιστρέφω και αναπνέω τον αέρα της Αττικής στο αεροδρόμιο, ακόμα και με τη μυρωδιά του καυσίμου των αεροπλάνων. Ζούμε σε μια καταπληκτική χώρα με πανέμορφα και προσιτά βουνά, νησιά και θάλασσες. Τις περισσότερες μέρες έχει ήλιο που σου ανοίγει

την καρδιά και τη διάθεση. Το κλίμα μας σπάνια είναι ακραίο και, ακόμα και σε αυτές τις περιπτώσεις, το χιόνι ή ο καύσωνας είναι ευκαιρία χαράς. Επίσης έχω την τύχη να έχω εδώ πολύ καλούς φίλους και συναδέλφους.



Με τη διεθνή ομάδα του ερευνητικού [CROSSMINER](#) (2015)

Με αλλαγές που έχουν γίνει τα τελευταία 30 χρόνια είναι πια εύκολο να ζεις στην Ελλάδα και να είσαι πολίτης του κόσμου. Έχουμε διαβατήρια και νόμισμα που μας επιτρέπουν να κυκλοφορούμε και να εργαζόμαστε εύκολα σε όλη την Ευρωπαϊκή Ένωση. Το διαδίκτυο και οι υποδομές υπολογιστικού νέφους μας επιτρέπουν να εργαζόμαστε από μακριά. Ζώντας την Αθήνα μπορώ να επικοινωνώ με ηλ-ταχ ή με τηλεδιάσκεψη με συναδέλφους σε όλο τον κόσμο, να διαβάζω επιστημονικές εργασίες την ώρα που εκδίδονται, να διευθύνω το κύριο διεθνές επιστημονικό περιοδικό για επαγγελματίες του κλάδου μου, να [συμμετέχω σε επιτροπές προγραμμάτων διεθνών συνεδρίων](#) και να [εκδίδω βιβλία με διεθνείς εκδοτικούς οίκους](#). Γνωρίζω συναδέλφους μας που εργάζονται ή εργάστηκαν στην Ελλάδα για τα κεντρικά εταιριών όπως οι Oracle, Cisco,

RedHat και GitHub. Αυτά δεν ήταν δυνατό να γίνουν παλαιότερα.

Σίγουρα χρειάζεται περισσότερη δουλειά για να καταφέρεις εδώ πράγματα που ίσως στο εξωτερικό θα ήταν πολύ εύκολα. Όμως και εκεί τα πράγματα, αν και δεν είναι όσο προβληματικά όσο είναι εδώ, δεν είναι ρόδινα. Συνάδελφοι από το εξωτερικό μου μεταφέρουν και από τα μέρη τους παράπονα για γραφειοκρατία, πολιτικές έριδες, υποχρηματοδότηση και έλλειψη πόρων.

Και κάτι τελευταίο. Έχουμε στο εξωτερικό πολλούς Έλληνες επιστήμονες πληροφορικής (και άλλων κλάδων) παγκόσμιας εμβέλειας. Έχω βάλει στοίχημα να αποδείξω ότι μπορεί κανείς να κάνει στο χώρο μου πρώτης τάξης επιστημονική έρευνα βασισμένος στην Ελλάδα.



Με την ερευνητική ομάδα του Εργαστηρίου Επιχειρηματικής Αναλυτικής στο [Παγκόσμιο Συνέδριο Τεχνολογίας Λογισμικού \(Gothenburg, 2018\)](#)

**Σε ποιον τομέα της Πληροφορικής δείχνουν το μεγαλύτερο ενδιαφέρον σήμερα οι φοιτητές σας;**

Οι φοιτητές με τους οποίους συνεργάζομαι στο [Εργαστήριο Επιχειρηματικής Αναλυτικής](#) ενδιαφέ-



ρονται ιδιαίτερα για εφαρμοσμένη πληροφορική. Συγκεκριμένα ενδιαφέρονται για την τεχνολογία λογισμικού (τη συστηματοποίηση της ανάπτυξης λογισμικού με τη χρήση μεθόδων της μηχανικής), την ασφάλεια των πληροφοριακών συστημάτων, τη μηχανική μάθηση και τα υπολογιστικά συστήματα.

Μερικές δημοσιευμένες εργασίες που εκπονήσαμε φέτος στο εργαστήριο με προπτυχιακούς φοιτητές και υποψήφιους διδάκτορες αφορούν την [ανάλυση του χάσματος ανάμεσα στην εκπαίδευση στην πληροφορική και των αναγκών της βιομηχανίας](#), τη [χρήση μηχανικής μάθησης στην τεχνολογία λογισμικού](#), τη [διερεύνηση του αντίκτυπου που έχει η έρευνα της τεχνολογίας λογισμικού στην πράξη](#) και την [εύρεση σφαλμάτων μεταγλωττιστών που σχετίζονται με τον έλεγχο των τύπων](#).

**Εκτός από τη θητεία σας στην ακαδημαϊκή κοινότητα, έχετε εργαστεί στη Google και έχετε υπηρετήσει ως Γενικός Γραμματέας Πληροφοριακών Συστημάτων στο Υπουργείο Οικονομικών. Πιστεύετε πως η Πληροφορική και οι άνθρωποί της θα μπορούσαν να είναι ο καταλύτης σημαντικών αλλαγών στις παθογένειες που ταλανίζουν διαχρονικά τη χώρα μας;**

Η πληροφορική μπορεί όντως να βοηθήσει στην καλύτερη οργάνωση του κράτους και στην προσφορά υψηλότερης ποιότητας υπηρεσιών στους πολίτες. Το έχουμε δει στην πράξη με καινοτόμες υπηρεσίες που έχει θέσει σε παραγωγική λειτουργία τα τελευταία χρόνια το

Υπουργείο Ψηφιακής Διακυβέρνησης. Αντίστοιχα, οι επιχειρήσεις ψηφιοποιώντας τις λειτουργίες τους μπορούν να γίνουν πιο ευέλικτες και αποδοτικές. Όμως, όπως γράψαμε και στη [μελέτη για την ηλεκτρονική διακυβέρνηση](#) που εκπονήσαμε με τη ΔιαΝΕΟσις, από μόνη της η ψηφιοποίηση δεν αρκεί για να βελτιώσει δραστικά έναν προβληματικό οργανισμό. Χωρίς δομικές οργανωτικές αλλαγές, η εφαρμογή της πληροφορικής είναι σα να ασπρίσουμε εξωτερικά τους τοίχους ενός στάβλου: το εσωτερικό του θα παραμείνει δυσώδες.



**Ομιλία με τίτλο [«Τεχνικές ανταρτοπόλεμου στη δημόσια διοίκηση»](#) — TEDx Academy 2012**

Αυτό που χρειάζεται για να αλλάξει πραγματικά πρόσωπο το κράτος μας ή μια επιχείρηση είναι λειτουργικές και οργανωτικές βελτιώσεις με στόχο την αναβάθμιση των προσφερόμενων υπηρεσιών και του εργασιακού περιβάλλοντος. Ένας τρόπος για να επιτευχθεί αυτό είναι ο λεγόμενος [ψηφιακός μετασχηματισμός](#), δηλαδή η χρήση ψηφιακών τεχνολογιών με στόχο την αναβάθμιση της εμπειρίας των πολιτών (ή πελατών), των εσωτερικών διεργασιών, του ρόλου του κράτους (ή του επιχειρηματικού μοντέλου) και της οργανωτικής διάρθρωσης.



**Ως διευθυντής σύνταξης του περιοδικού IEEE Software με το εκδοτικό και συμβουλευτικό συμβούλιο (2018)**

Ας φέρουμε για παράδειγμα στο μυαλό μας το ηλεκτρονικό εισιτήριο που εισήχθη στα μέσα μαζικής μεταφοράς στην Αθήνα το 2017. Τα προϊόντα που αυτό υποστηρίζει ήταν και συνεχίζουν να είναι πέντε χρόνια αργότερα ακριβώς τα ίδια με τα χάρτινα που αντικατέστησε. Η ψηφιοποίηση δεν αξιοποιήθηκε για την εισαγωγή πιο ευέλικτων και αποδοτικών τρόπων χρέωσης, όπως θα ήταν μειωμένο κόμιστρο για μικρότερες αποστάσεις, διαφοροποίηση της τιμής στις ώρες αιχμής για εξισορρόπηση της επιβατικής κίνησης, δυναμική ενημέρωση των επιβατών σχετικά με την κοσμοσυρροή, ή αυτόματη οροφή της χρέωσης στο ύψος της ημερήσιας μετά από έναν αριθμό μετακινήσεων. Επίσης, δεν αξιοποιήθηκε η ασύρματη τεχνολογία NFC στις μπάρες προκειμένου να δοθεί η δυνατότητα ανοίγματος της μπάρας με τη χρήση αντίστοιχης πιστωτικής κάρτας, χωρίς να απαιτείται αγορά εισιτηρίου.

Μια άλλη χαρακτηριστική περίπτωση αφορά την αναποτελεσματικότητα του συστήματος

απονομής της δικαιοσύνης στη χώρα μας και τις μεγάλες καθυστερήσεις που σημειώνονται στην εκδίκαση των υποθέσεων. Οι δυσλειτουργίες αυτές εμποδίζουν την επιχειρηματικότητα, προάγουν την ανομία και μειώνουν την εμπιστοσύνη των πολιτών στο κράτος δικαίου. Τα αλληπάλληλα έργα ψηφιοποίησης της δικαιοσύνης που έχουν πραγματοποιηθεί την τελευταία εικοσαετία ελάχιστα μπόρεσαν να βελτιώσουν την κατάσταση. Ο λόγος γι' αυτό είναι ότι για την επίλυση αυτών των προβλημάτων απαιτούνται σύνθετες δομικές αλλαγές που δε σχετίζονται απαραίτητα με την πληροφορική.



**Με την ερευνητική ομάδα του Εργαστηρίου Επιχειρηματικής Αναλυτικής στην Πάρνηθα (2019)**

Ο δρόμος των απαραίτητων μεταρρυθμίσεων ξεκινά από την αξιοκρατία, που θα φέρει σε θέσεις ευθύνης ανθρώπους που θα μπορούν πραγματικά να την αναλάβουν, αντί να κρύβονται πίσω από διατάξεις. Συνεχίζει με μεταβίβαση αρμοδιοτήτων, ώστε οι αρμόδιοι δημόσιοι λειτουργοί να μπορούν να αποφασίζουν με βάση την ουσία και όχι τον τύπο. Περιλαμβάνει την ενίσχυση της λογοδοσίας, της αξιολόγησης, του

ανταγωνισμού, καθώς και της δημόσιας διάθεσης δεδομένων· αυτά είναι τα μέσα που επιτρέπουν σε όλους τους ενδιαφερόμενους να κρίνουν και να κρίνονται. Διατρέχεται από τη σταδιακή εδραίωση άτυπων κανόνων κοινωνικής συμπεριφοράς, σεβασμού και ανεκτικότητας. Απαιτεί ενίσχυση της παιδείας, ώστε να παράγει πολίτες τις κατάλληλες γνώσεις, την απαιτούμενη ευθυκρισία και την υψηλή αίσθηση του καθήκοντος.



**Γράφοντας κώδικα για την ανάλυση ποιότητας λογισμικού με τον (τότε) υποψήφιο διδάκτορα, τώρα διευθυντή έρευνας στα Endor Labs και αναπληρωτή καθηγητή στο Delft University of Technology Γ. Γούσιο (2008)**

**Η πανδημία έφερε ραγδαία είσοδο της τεχνολογίας σε ακόμα περισσότερους τομείς της ζωής μας. Πέρα από τα αναμφισβήτητα οφέλη, συμμαρρίζετε τις ανησυχίες για όσα συζητούνται σχετικά με την τεχνητή νοημοσύνη;**

Υπάρχουν πολλοί λόγοι για τους οποίους οι άνθρωποι μπορεί να ανησυχούν για την ανάπτυξη της τεχνητής νοημοσύνης. Μερικές από τις πιο συχνά αναφερόμενες ανησυχίες είναι οι εξής.

**Ανεργία:** Καθώς οι τεχνολογίες τεχνητής νοημοσύνης γίνονται πιο προηγμένες και ικανές

να εκτελούν ένα ευρύτερο φάσμα εργασιών, υπάρχει ο φόβος ότι θα αντικαταστήσουν τους ανθρώπινους εργατές σε πολλούς κλάδους, οδηγώντας σε εκτεταμένη ανεργία και οικονομική αναστάτωση.

**Προκαταλήψεις:** Τα συστήματα τεχνητής νοημοσύνης συνήθως εκπαιδεύονται σε σύνολα δεδομένων που αντικατοπτρίζουν τις προκαταλήψεις των ανθρώπων που τα δημιουργούν. Εάν αυτές οι προκαταλήψεις δεν εντοπιστούν και δεν αντιμετωπιστούν, μπορούν να διαιωνιστούν και να ενισχυθούν από το σύστημα τεχνητής νοημοσύνης, οδηγώντας σε άδικο και μεροληπτικά αποτελέσματα.

**Ατυχήματα:** Τα συστήματα τεχνητής νοημοσύνης που χρησιμοποιούνται για τη λήψη αποφάσεων σε καταστάσεις υψηλού κινδύνου, όπως αυτοοδηγούμενα αυτοκίνητα ή στρατιωτικά μη επανδρωμένα αεροσκάφη, θα μπορούσαν ενδεχομένως να προκαλέσουν βλάβη σε περίπτωση δυσλειτουργίας ή ακατάλληλης χρήσης.

**Κακόβουλη χρήση:** Οι προηγμένες τεχνολογίες τεχνητής νοημοσύνης θα μπορούσαν να χρησιμοποιηθούν από άτομα ή οργανισμούς για τη διεξαγωγή κακόβουλων δραστηριοτήτων, όπως πειρατεία, επιθέσεις στον κυβερνοχώρο ή εκστρατείες παραπληροφόρησης.

**Παραβίαση προσωπικών δεδομένων:** Τα συστήματα τεχνητής νοημοσύνης που είναι σε θέση να επεξεργάζονται μεγάλους όγκους προσωπικών δεδομένων θα μπορούσαν να χρησιμοποιηθούν για να παραβιάσουν τα δικαιώματά που σχετίζονται με την προστασία των προσωπικών δεδομένων.

**Κοινωνικός διχασμός:** Η ανάπτυξη τεχνολογιών τεχνητής νοημοσύνης θα μπορούσε να επιδεινώσει τις υπάρχουσες κοινωνικές και οικονομικές διαφορές, καθώς ορισμένες ομάδες μπορεί να έχουν πρόσβαση και να επωφεληθούν από την τεχνολογία, ενώ άλλες όχι.



[Προσομοίωση του Μηχανισμού των Αντικυθήρων](#)  
 ΣΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΠΟΛΟΓΙΣΤΗ OLPC (2007)

**Ηθικά ζητήματα:** Τα συστήματα τεχνητής νοημοσύνης έχουν σχεδιαστεί για να λαμβάνουν αποφάσεις με βάση τα δεδομένα που τους παρέχονται. Ωστόσο, τα δεδομένα που χρησιμοποιούν τα συστήματα τεχνητής νοημοσύνης μπορεί να είναι μεροληπτικά ή ελλιπή, οδηγώντας σε ανήθικα ή άδικο αποτελέσματα. Για παράδειγμα, ένα σύστημα τεχνητής νοημοσύνης που χρησιμοποιείται στο σύστημα της ποινικής δικαιοσύνης μπορεί να λαμβάνει αποφάσεις με βάση μεροληπτικά

δεδομένα, με αποτέλεσμα την άνιση μεταχείριση διαφορετικών ομάδων ανθρώπων.

**Έλλειψη λογοδοσίας:** Επειδή τα συστήματα τεχνητής νοημοσύνης είναι συχνά σχεδιασμένα να λειτουργούν αυτόνομα, μπορεί να είναι δύσκολο να κατανοήσουμε πώς λαμβάνουν αποφάσεις και αναλαμβάνουν ενέργειες. Αυτή η έλλειψη διαφάνειας και λογοδοσίας μπορεί να δυσχεράνει την ανάληψη ευθύνης των συστημάτων τεχνητής νοημοσύνης για τις ενέργειές τους, γεγονός που θα μπορούσε να οδηγήσει σε επιβλαβείς ή ανεπιθύμητες συνέπειες.

Συμπερασματικά, ενώ η τεχνητή νοημοσύνη έχει τη δυνατότητα να αποφέρει πολλά οφέλη, είναι σημαντικό να εξεταστούν προσεκτικά και να αντιμετωπιστούν οι πιθανοί κίνδυνοι και οι αρνητικές επιπτώσεις της ανάπτυξής της.

**Σημείωση:** δημιούργησα το παραπάνω κείμενο χρησιμοποιώντας δύο συστήματα τεχνητής νοημοσύνης. Έθεσα την ερώτηση «Why should we be worried about AI?» στο σύστημα [ChatGPT](#) (δύο φορές) και μετέφρασα τις απαντήσεις στα ελληνικά με τη χρήση του [Google Translate](#). Το αγγλικό κείμενο του ChatGPT ήταν άψογο. Χρειάστηκε όμως να επιμεληθώ ελαφρώς την ελληνική μετάφραση για την κάνω πιο ευανάγνωστη. Η ειρωνεία είναι ότι το ChatGPT διεκπεραίωσε το δημιουργικό τμήμα της δουλειάς και εγώ ανέλαβα τη ρουτίνα της επιμέλειας του κειμένου.





**Ομιλία σε εκδήλωση του Ελληνικού Μουσείου Πληροφορικής (2014)**

**Πιστεύετε ισχυρά στην κουλτούρα του ελεύθερου και ανοικτού λογισμικού και έχετε διατελέσει Πρόεδρος στον Οργανισμό Ανοιχτών Τεχνολογιών (ΕΕΛΛΑΚ). Θεωρείτε πως εκτός από τα σημαντικά επιτεύγματα στον κλάδο της Πληροφορικής, θα μπορούσε η φιλοσοφία της Ανοιχτότητας να εξαπλωθεί και να λειτουργήσει αποτελεσματικά και σε άλλους τομείς;**

Με βάση τις αρχές της ανοιχτότητας θα πρέπει τα δημόσια, μη προσωπικά, δεδομένα, να είναι ελεύθερα προσβάσιμα απ' όλους. Η αρχή αυτή ισχυροποιήθηκε σημαντικά στη χώρα μας με τον εξαιρετικά προοδευτικό νόμο 4305/2014 που ορίζει ότι τα έγγραφα, οι πληροφορίες και τα δεδομένα του δημόσιου τομέα πρέπει κατά κανόνα να διατίθενται ελεύθερα για κάθε χρήση μέσω του διαδικτύου. Δυστυχώς, ενώ θα έπρεπε να χτίσουμε τις πληροφοριακές υποδομές που να τον κάνουν πράξη — να φροντίσουμε δηλαδή κάθε υπάρχον και νέο πληροφοριακό σύστημα να διαθέτει σε όλους μας, με ανοικτό τρόπο, τα δημόσια δεδομένα που τηρεί — αυτό δεν έχει γίνει. Αυτό είναι πολύ κρίμα, διότι η ανοιχτότητα και η διαφάνεια μπορούν να υπηρετήσουν πολλαπλά τη χώρα μας.

Μπορούμε εύκολα να καταλάβουμε ότι η διαφάνεια στα δημόσια δεδομένα συμβάλλει σημαντικά στην **καταπολέμηση της διαφθοράς**. Αν η σειρά προτεραιότητας και η παροχή υπηρεσιών από παιδικούς σταθμούς, σχολεία, νοσοκομεία, πολεοδομίες, είναι ανοιχτή και προσβάσιμη απ' όλους, μειώνονται δραστικά οι τρόποι με τους οποίους κάποιος μπορεί να διασφαλίσει προνομιακή μεταχείριση με αθέμιτο τρόπο. Αντίστοιχα, αν δημοσιεύονται αυτόματα μέσω πληροφοριακού συστήματος οι έλεγχοι που προγραμματίσει και εκτέλεσε κάθε δημόσια αρχή καθώς και τα αποτελέσματά τους σε επίπεδο ελεγκτή, τότε θα αποκαλύπτονταν οι λίγοι επίορκοι υπάλληλοι που ντροπιάζουν τον κλάδο τους.



**Ομιλία στο Παγκόσμιο Συνέδριο Τεχνολογίας Λογισμικού (2018)**

Με διαφάνεια στα δημόσια δεδομένα δημιουργούνται προϋποθέσεις για **αποτελεσματικότερη άσκηση της πολιτικής**. Οι ψηφοφόροι, τα κόμματα και φορείς της κοινωνίας των πολιτών μπορούν να γνωρίζουν και να επικαλούνται τα στοιχεία που δικαιολογούν συγκεκριμένες πολιτικές.

Μπορούμε λ.χ. να ξέρουμε πόσο κοστίζει μια διανυκτέρευση ασθενούς ή μια επέμβαση σε κάθε δημόσιο νοσοκομείο, ποιοι δικαστές βγάζουν αποφάσεις που επικυρώνονται ή εξαφανίζονται μετά από έφεση, πώς αξιολογούν τους καθηγητές τους οι φοιτητές σε κάθε τμήμα, πόσες και τι είδους κλήσεις έδωσε κάθε τροχονόμος, πόσο συχνά γίνεται η αποκομιδή απορριμμάτων ανά δήμο και ποιες αιτήσεις για άσυλο γίνονται δεκτές κάθε χρόνο.

Τέλος, αν τα δεδομένα και τα αποθετήρια ψηφιακού περιεχόμενου που υπάρχουν σ' όλα τα πληροφοριακά συστήματα του δημοσίου είναι ελεύθερα διαθέσιμα, τότε αυτά μπορούν να χρησιμοποιηθούν από επιχειρήσεις για την **παροχή υπηρεσιών πρόσθετης αξίας**. Αυτή η πρακτική ευνοεί την καινοτομία και την ανάπτυξη. Επίσης, μέσω της φορολογίας και των εισφορών που αντιστοιχούν στην οικονομική δραστηριότητα, αξιοποιούνται οι πολύτιμοι πόροι που έχουν δημιουργηθεί με χρήματα των φορολογουμένων. Ως ένα παράδειγμα, σκεφτείτε την εφαρμογή της ηλεκτρονικής συνταγογράφησης. Αν τα δεδομένα και οι εφαρμογές του Πρωτοβάθμιου Εθνικού Δικτύου Υγείας (ΠΕΔΥ), της Ηλεκτρονικής Διακυβέρνησης Κοινωνικής Ασφάλισης (ΗΔΙΚΑ) και του Εθνικού Οργανισμού Φαρμάκων ήταν ανοικτά διαθέσιμα, τότε ελληνικές επιχειρήσεις θα μπορούσαν να αναπτύξουν εύχρηστες και έξυπνες εφαρμογές που να συνδυάζουν π.χ. τη συνταγογράφηση με το φάκελο του ασθενούς και τα ραντεβού για τους γιατρούς, ή την παραγγελιοληψία για τα φαρμακεία. Κάποια από αυτές τις επιχειρήσεις, βοηθούμενη από τη διαφάνεια, την ανοιχτότητα και τη

διαλειτουργικότητα των πληροφοριακών συστημάτων της ηλεκτρονικής διακυβέρνησης, θα μπορούσε να είναι ο αυριανός παγκόσμιος κυρίαρχος στο συγκεκριμένο χώρο.



**Ομιλία ως Πρόεδρος του Τμήματος Διοικητικής Επιστήμης και Τεχνολογίας σε τελετή αναγόρευσης της Καθηγήτριας του LSE κυρίας Χρυσάνθης Αυγέρου σε Επίτιμη Διδάκτορα (2018)**

### **Ποιον άνθρωπο της Επιστήμης των Υπολογιστών αληθινά θαυμάζετε; (Είτε ιστορικό πρόσωπο, είτε σύγχρονο)**

Θα αναφέρω έναν άνθρωπο που όχι μόνο θαυμάζω απεριόριστα, αλλά είχα την τύχη να γνωρίσω και να συνεργαστώ μαζί του: τον μαθηματικό, προγραμματιστή και μηχανικό Doug McIlroy. Ο McIlroy εργάστηκε στα διάσημα AT&T Bell Laboratories από το 1958 μέχρι το 1997. Την περίοδο 1965—1986 διεύθυνε το Τμήμα Έρευνας Υπολογιστικών Τεχνικών, όπου αναπτύχθηκαν μεταξύ άλλων το λειτουργικό σύστημα Unix, οι γλώσσες προγραμματισμού C, C++ και awk, και πολλά άλλα πρωτοποριακά εργαλεία προγραμματισμού.

Σε μια έρευνα που κάναμε για την [εξέλιξη της αρχιτεκτονικής του λειτουργικού συστήματος Unix](#) στο μισό αιώνα της ζωής του, ανακάλυψα

ότι ο McIlroy είχε διατυπώσει από το 1964 τις βασικές αρχές των σωληνώσεων (pipelines) που θα γίνονταν βασικό στοιχείο του Unix σχεδόν δέκα χρόνια αργότερα.

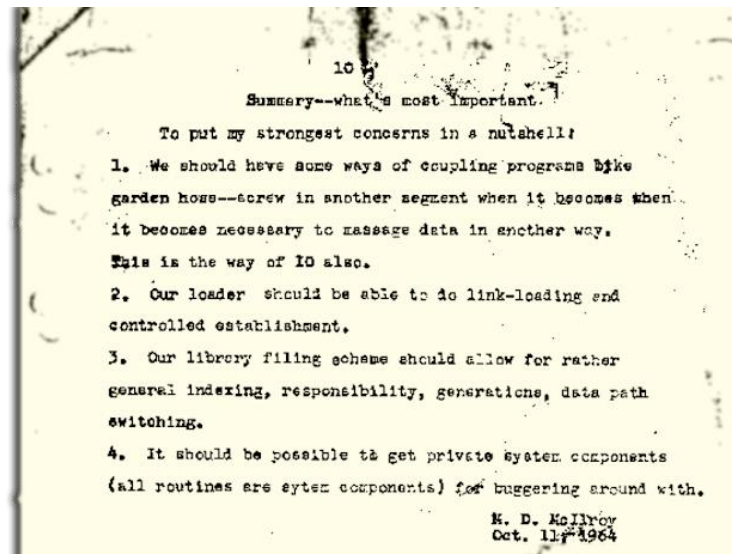


**Douglas McIlroy (2011)**

Φωτογραφία: Denise Panyik-Dale · [CC BY 2.0](#)

Εργαλεία και διασυνδέσεις τους που βασίζονται σε σωληνώσεις μάς επιτρέπουν μέχρι και σήμερα να [επεξεργαζόμαστε δεδομένα κάθε είδους με εξαιρετικά ευέλικτο, αποδοτικό και ευσύνητο τρόπο](#). Μεταξύ άλλων ο McIlroy έχει συνεισφέρει στο σχεδιασμό πολλών σημαντικών γλωσσών προγραμματισμού και είναι πρωτεργάτης των πρακτικών της ενθυλάκωσης και επαναχρησιμοποίησης λογισμικού — του βασικού τρόπου με τον οποίο μπορούμε σήμερα να υλοποιούμε μεγάλα και σύνθετα έργα πληροφορικής. Έχει επίσης δουλέψει σε

μεταγλωττιστές, κανονικές εκφράσεις, ασφάλεια υπολογιστών, χαρτογραφία, γραφικά, διαχείριση μνήμης και την τεκμηρίωση του Unix. Παράλληλα με την πλούσια ερευνητική του δράση και τις διοικητικές του υποχρεώσεις, υλοποίησε πολλά κομβικά εργαλεία του Unix που χρησιμοποιούνται ευρύτατα μέχρι σήμερα. Αναφέρω χαρακτηριστικά τις εντολές *diff*, *sort*, *join*, *tsort* και *tr*. Τέλος έχει υπηρετήσει από σημαντικές θέσεις την επιστημονική και ερευνητική κοινότητα της πληροφορικής μέσω του οργανισμού [Association for Computing Machinery](#). Ο τρόπος που συνδύασε επιστημονική έρευνα με κατασκευή υπολογιστικών συστημάτων αποτελεί για μένα πρότυπο και οδηγό.



**Σημείωμα του McIlroy όπου προδιαγράφει την ιδέα των σωληνώσεων (1964)**

Την περίοδο 2014–2016 επικοινωνούσα μαζί του σχετικά με έναν πιο [σύνθετο τρόπο διασύνδεσης προγραμμάτων στο φλοιό του Unix](#) που σχεδιάζαμε. Μου έκαναν εντύπωση η απλόχερη διάθεσή του να βοηθήσει, η οξυδέρκειά του και το βάθος της σκέψης του. Όταν λάμβανα ένα μήνυμά του, χρειαζόμουν πολλές ώρες για να



αναλύσω και να κατανοήσω πλήρως κάθε παράγραφο των σχολίων του. Συχνά με προέτρεπε προς κατευθύνσεις που ήταν στα όρια των ικανοτήτων μου.

Από το 1997 ο αειθαλής McIlroy είναι επισκέπτης καθηγητής στο Τμήμα Πληροφορικής του [Dartmouth College](#), και συνεχίζει παράλληλα να συνεισφέρει με διάφορους τρόπους στην επιστημονική κοινότητα, δείχνοντας σε όλους μας πώς η επιστημοσύνη θα πρέπει να συνδυάζεται με κοινωνική προσφορά.

### **Ποια συμβουλή θα δίνετε σήμερα σ' έναν φοιτητή ή νέο απόφοιτο της Πληροφορικής;**

«Έχεις τη μοναδική τύχη να ζεις σε μια εποχή που όλη η γνώση της ανθρωπότητας είναι προσβάσιμη σε εσένα. Παράλληλα έχεις στα χέρια σου υπολογιστικά εργαλεία που πριν πενήντα χρόνια τα μεγαλύτερα ερευνητικά κέντρα του κόσμου δεν θα μπορούσαν ούτε να τα ονειρευτούν. Εκμεταλλεύσου αυτές τις δυνατότητες για να επεκτείνεις τις γνώσεις σου προς τις κατευθύνσεις που σε ενδιαφέρουν. Μάθε καινούριες γλώσσες προγραμματισμού, βιβλιοθήκες, εργαλεία και εφαρμογές. Επίσης, έχεις την τύχη να δουλεύεις σε έναν τεχνολογικό κλάδο όπου τα σχέδια και η υλοποίηση πολλών εξαιρετικά σημαντικών τεχνουργημάτων είναι ανοιχτά διαθέσιμα — ως ελεύθερο λογισμικό ή λογισμικό ανοιχτού κώδικα (ΕΛ/ΛΑΚ). Εκμεταλλεύσου και αυτή τη δυνατότητα για να καταλάβεις σε βάθος τις τεχνολογίες που σε ελκύουν. [Διάβασε τον κώδικα](#) για να καταλάβεις τη δομή του και τις τεχνικές που χρησιμοποιεί. Προχώρα ένα βήμα παρακάτω, [συνεισφέροντας σε έργα ΕΛ/ΛΑΚ](#) που χρησιμοποιείς ή θέλεις να

δεις να βελτιώνονται. Έτσι μπορεί να έχεις την ευκαιρία να συνεργαστείς με τους μελλοντικούς συναδέλφους σου απ' όλο τον κόσμο και να γνωρίσεις από πρώτο χέρι τις πιο σύγχρονες διεργασίες ανάπτυξης λογισμικού — πρακτικές που στο παρελθόν ήταν συχνά εμπορικά μυστικά μεγάλων εταιριών του χώρου. Επιπλέον, ως πληροφορικός έχεις την ικανότητα να χρησιμοποιείς τα εργαλεία του κλάδου μας για να βελτιώνεις [τη δική σου παραγωγικότητα και αποδοτικότητα](#). Βάλε ως στόχο να αναβαθμίζεις διαρκώς τον τρόπο που δουλεύεις εσύ και η ομάδα σου με τη χρήση της πληροφορικής. Τέλος, αναλογίσου αυτούς στους οποίους χρωστάς ευγνωμοσύνη για ό,τι σου δόθηκε η δυνατότητα να καταφέρεις, και προσπάθησε να το ανταποδώσεις προσφέροντας πίσω στην κοινωνία αυτά που σου προσφέρθηκαν.»

*Ευχαριστώ θερμά για την πρόσκληση της συνέντευξης και τη φιλοξενία. Ελπίζω να μη σας κούρασα. Περισσότερες πληροφορίες για πολλά από τα παραπάνω θέματα μπορείτε να βρείτε και [στην οικοσελίδα μου](#).*



**Από τα γραφεία του πανεπιστημίου στην οδό Ευελπίδων στο κεντρικό κτήριο της οδού Πατησίων μέσω του Πεδίου το Άρεως (2005)**



# ✓ Peopleware

// Επιμέλεια στήλης: **Νεκτάριος Μουμουτζής**

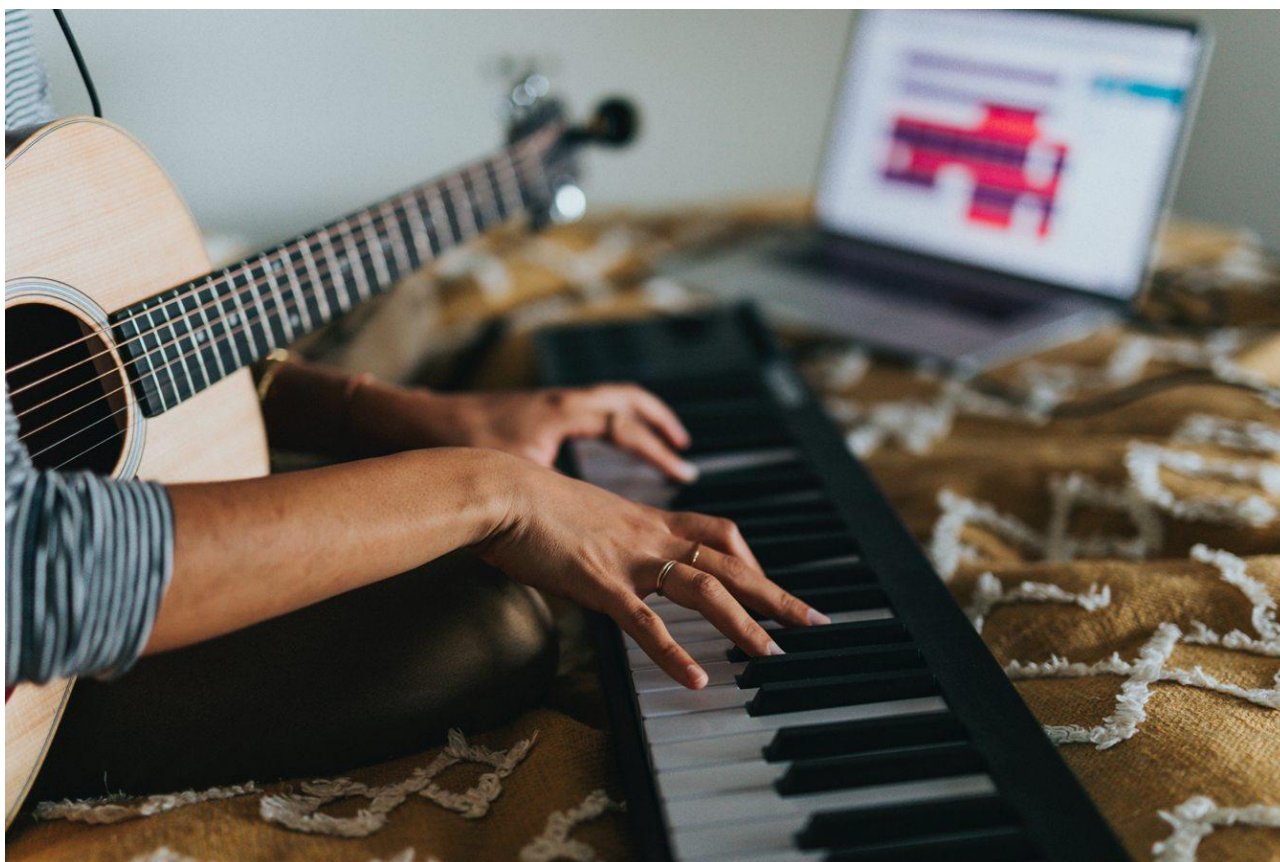


Photo by [Soundtrap](#)

Μια νέα στήλη ξεκινά από το παρόν τεύχος του Πληροφορικού. Μια στήλη που στόχο έχει να αναδείξει το ανθρώπινο πρόσωπο της Πληροφορικής. Ή, αν το προτιμάτε, τις ψυχοθεραπευτικές της δυνατότητες όταν καλλιεργεί και ενισχύει την δημιουργικότητα. Η στήλη θα προσπαθήσει να αναδείξει αυτή τη διάσταση της Πληροφορικής μέσα από ανθρώπινες ιστορίες που λειτουργούν ως παραβολές αφήνοντας τον αναγνώστη να βγάλει τα δικά του συμπεράσματα. Κάποιες από τις ιστορίες αυτές είναι πραγματικά περιστατικά με τροποποίηση ονομάτων προσώπων και

άλλων λεπτομερειών για να μην αποκαλύπτονται ευαίσθητα προσωπικά δεδομένα. Άλλες ιστορίες θα βασίζονται στη μυθοπλασία...

Αν έχετε κι εσείς κάποια ιστορία που αναδεικνύει το ανθρώπινο πρόσωπο της Πληροφορικής, μπορείτε να επικοινωνήσετε με τον επιμελητή της στήλης στη διεύθυνση [nmoumoutzis@tuc.gr](mailto:nmoumoutzis@tuc.gr) για να τη μοιραστείτε με τους αναγνώστες του Πληροφορικού.

## ☆ Η Πληροφορική κερδίζει μια ταλαντούχο μουσικό!

Η Ιωάννα ήταν μια από τις καλύτερες μαθήτριες της τάξης της. Είχε ακολουθήσει τη θετική κατεύθυνση αν και ο πραγματικός της προορισμός, όπως είχε καταλάβει από μικρή, ήταν η μουσική. Όταν ήρθε η ώρα να δηλώσει τα πανεπιστημιακά τμήματα της επιλογής της μετά τις πανελλήνιες εξετάσεις, ακολουθώντας τη «μόδα» των ημερών, δήλωσε πρώτα τα τμήματα της Πληροφορικής και έτσι βρέθηκε πρωτοετής να μελετά Λογική Σχεδίαση και Προγραμματισμό σε C... Από τις πρώτες μέρες στα αμφιθέατρα βρέθηκε να αντιμετωπίζει μια κρίση ταυτότητας:

- Τι κάνω εγώ εδώ; αναρωτιόνταν. Ποτέ δεν θα τα καταλάβω αυτά τα πράγματα, εγώ είμαι γεννημένη μουσικός.

Ενώ είχε αυτούς τους προβληματισμούς, συνέχισε να παρακολουθεί τα μαθήματα και να κάνει τις ασκήσεις της, πάντα με έναν πολύ ιδιαίτερο δικό της τρόπο χωρίς να ακολουθεί την πεπατημένη των μεθόδων που δίδασκαν οι καθηγητές της. Πάντα με σωστό τελικό αποτέλεσμα!

Καθώς το πρώτο εξάμηνο τελείωνε, σε μια εξέταση στον προγραμματισμό, ο εξεταστής,

αφού έριξε μια ματιά στον κώδικα που είχε παραδώσει, την ξάφνιασε ρωτώντας την:

- Έχεις κάποιο χόμπι; Τι σου αρέσει να κάνεις στον ελεύθερο χρόνο σου; Ασχολείσαι με κάτι καλλιτεχνικό;

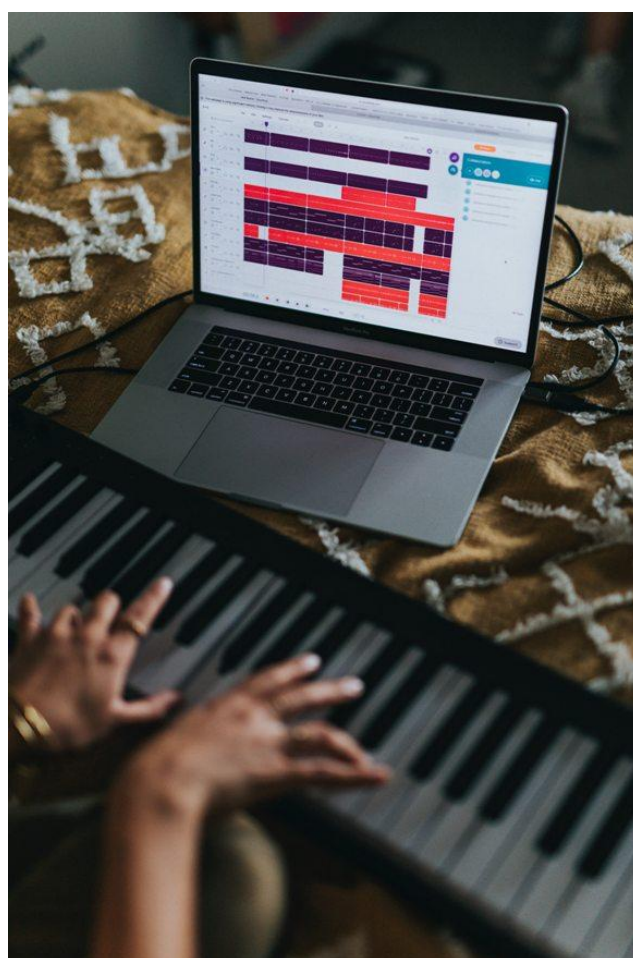


Photo by [Soundtrap](#)

- Είμαι μουσικός! του απάντησε με ενθουσιασμό. Συνθέτω κιόλας!

- Λοιπόν, άκουσε τι θα σου πω. Ο κώδικας που έχεις γράψει παράγει το σωστό αποτέλεσμα αλλά δεν ακολουθεί τους κανόνες που έχουμε πει στο μάθημα. Είναι, πώς να σου το πω, σαν μακαρονάδα, spaghetti code στα αγγλικά. Κανονικά δεν θα έπρεπε να σου βάλω προβιβάσιμο βαθμό. Ωστόσο, είσαι τυχερή γιατί πρόσφατα διάβασα μια μελέτη(\*\*) που τεκμηριώνει ότι φοιτητές που έχουν δημιουργικό ταλέντο καθώς και οι κοπέλες, σε μεγάλο ποσοστό, γράφουν τέτοιο κώδικα καθώς προσεγγίζουν τον προγραμματισμό όπως ο καλλιτέχνης τη δημιουργία ενός έργου τέχνης. Η Πληροφορική έχει ανάγκη από δημιουργικά ταλέντα όπως εσύ και δεν θα ήθελα να σε απογοητεύσω βαθμολογώντας σε όπως συνήθως. Ωστόσο, πρόσεξε γιατί άλλοι συνάδελφοι μπορεί να μην σε αντιμετωπίσουν όπως εγώ.

- Ευχαριστώ πολύ! είπε η Ιωάννα. Η αλήθεια είναι ότι αμφιβάλλω πολύ αν έκανα τη σωστή επιλογή να σπουδάσω Πληροφορική. Η δική μου επιθυμία είναι να ασχοληθώ με τη μουσική. Αυτό θέλω να κάνω στη ζωή μου!

- Τότε έχεις κάνει μια εξαιρετική επιλογή! αντέτεινε ο εξεταστής. Μπορείς να κάνεις καταπληκτικά πράγματα ως μουσικός αν μάθεις να αξιοποιείς τους υπολογιστές. Θα σου στείλω στο email σου κάποιες σελίδες να δεις τι μπορείς να κάνεις. Μην έχεις καμία αμφιβολία ότι μπορείς να συνδυάσεις τη μουσική με τους υπολογιστές και μάλιστα θα μπορείς να κάνεις πράγματα που δεν θα μπορούσες να κάνεις αν επέλεγες να σπουδάσεις μουσική.

Η Ιωάννα, κατάφερε να περάσει το συγκεκριμένο μάθημα, όμως, σε άλλα μαθήματα αντιμετώπισε δυσκολίες, όπως την είχε προειδοποιήσει ο εξεταστής. Ωστόσο, με υπομονή και επιμονή κατάφερε να ολοκληρώσει τις σπουδές της και να αντιληφθεί τις δυνατότητες που είχε ως μουσικός-πληροφορικός. Είναι μάλιστα χαρακτηριστικό το γεγονός ότι στη διπλωματική της εργασία ανέπτυξε ένα ευφυές σύστημα μουσικής σύνθεσης με νευρωνικά δίκτυα! Πλέον βλέπει τη μουσική και την Πληροφορική με άλλα μάτια... Η Πληροφορική κέρδισε ένα δημιουργικό ταλέντο και η μουσική απέκτησε μια Πληροφορικό!

#### **Αναφορές:**

(\*) Ο όρος *reopleware*, σύμφωνα με το σχετικό λήμμα της αγγλικής Wikipedia, αναφέρεται σε μία από τις τρεις βασικές πτυχές της τεχνολογίας των υπολογιστών, ενώ οι άλλες δύο είναι το υλικό (*hardware*) και το λογισμικό (*software*). Ο όρος *reopleware* μπορεί να αναφέρεται σε οτιδήποτε έχει να κάνει με το ρόλο των ανθρώπων στην ανάπτυξη ή τη χρήση συστημάτων λογισμικού και υλικού υπολογιστών.

(\*\*) Sherry Turkle and Seymour Papert: "Epistemological Pluralism and the Reevaluation of the Concrete", *Journal of Mathematical Behavior*, Vol. 11, No.1, in March, 1992, pp. 3-33; *Constructionism*, I. Harel & S. Papert, Eds. (Ablex Publishing Corporation, 1991), pp.161-191; and *SIGNS: Journal of Women in Culture and Society*, Autumn 1990, Vol. 16 (1). Διαθέσιμο ηλεκτρονικά από τη διεύθυνση: <https://web.media.mit.edu/>



## ✓ Φόρεσε το άσπρο καπέλο του χάκερ\*

// Γράφει ο Γιάννης Φαρσάρης



Photo by [hmm 001](#)

Οι ταινίες και τα ΜΜΕ έχουν φορτίσει αρνητικά τη λέξη “hacker”, αποδίδοντάς της στοιχεία παραβατικότητας, όμως παλιά ο όρος σήμαινε αυτόν που φτιάχνει επίπλα πελεκώντας το ξύλο με τσεκούρι. Εντάξει, οι δημοσιογράφοι αρέσκονται σε σενάρια συνωμοσίας και έκαναν διάσημους σταρ τον Κέβιν Μίτνικ (έγραψε ιστορία με το σύνθημα “FreeKevin”), τον Άντριαν Λάμο και άλλους πολλούς, όπως και σήμερα την ομάδα Αποηγτους. Όμως εδώ θα χρησιμοποιήσουμε τον όρο με την αυθεντική του σημασία. Η λέξη έχει την έννοια του εφευρέτη, αυτού που ασχολείται έτσι ώστε να ανακαλύψει το πώς λειτουργεί ένα σύστημα και να το βελτιώσει ή να το αλλάξει τροποποιώντας το. Η αυθεντική υποκουλτούρα των χάκερς της δεκαετίας του 1960 είχε προέλθει από κύκλους της Επιστήμης Υπολογιστών —ιδιαίτερα της τεχνητής νοημοσύνης— στις ΗΠΑ, αρχικά στο Τεχνολογικό Ινστιτούτο της Μασαχουσέτης και μεταγενέστερα σε άλλα πανεπιστημιακά ιδρύματα, όπως το Στάνφορντ και το Πρίνστον. Όταν οι πράξεις τους είναι κακόβουλες αποκαλούνται “black hat hackers” ή “crackers”. Ο όρος “black hat” προέρχεται από το χρώμα του καπέλου που



φορούσαν οι κακοί χαρακτήρες στα γουέστερν της δεκαετίας του '50. Όμως εδώ θα αναφερθούμε στους "white hat hackers" και στους "grey hat hackers" ή "hacktivists". Δεν υστερούν καθόλου σε τεχνικές γνώσεις από τους σκληρούς crackers, όμως όλες τους οι ενέργειες υπακούν σε αυστηρούς κώδικες ηθικής (hacker ethics) και γι' αυτό ονομάζονται και "ηθικοί χάκερς".



Photo by [Hugo Jehanne](#)

Το 1984 ο Στίβεν Λέβι έγραψε το βιβλίο «*Χάκερς: οι ήρωες της Επανάστασης των Υπολογιστών*», όπου και ταξινομήσε και ανέλυσε τους σημαντικότερους κώδικες ηθικής τους:

1) Η γνώση πρέπει να είναι ελεύθερη.

2) Η πρόσβαση σε υπολογιστές και σε ο,τιδήποτε μπορεί να σε διδάξει κάτι σχετικά με τον τρόπο με τον οποίο λειτουργεί ο κόσμος, πρέπει να είναι απεριόριστη και συνολική.

3) Ένας χάκερ είναι δύσπιστος σε όλες τις μορφές εξουσίας.

4) Ένας χάκερ θα πρέπει να κρίνεται σύμφωνα με τις ικανότητές του στο χάκινγκ και όχι με κριτήρια την ηλικία του ή το πτυχίο του.

5) Ένας χάκερ μπορεί να δημιουργήσει τέχνη και ομορφιά μέσω ενός υπολογιστή.

6) Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο.

Διαβάζοντας αυτές τις ηθικές αρχές, είναι δύσκολο να διαφωνήσει κανείς. Το χάκινγκ δεν χρειάζεται καν να αφορά υπολογιστές. Ο θρύλος Ρίτσαρντ Στόλλμαν λέει: «Το χάκινγκ σαν μια γενική έννοια, είναι μια στάση απέναντι στη ζωή. Τι έχει πλάκα για σένα; Αν το να ανακαλύπτεις παιγνιωδώς έξυπνους τρόπους που θεωρούνταν ότι ήταν αδύνατοι παλιά έχει πλάκα, τότε είσαι ένας χάκερ». Το 2007 όλος ο (δυτικός τουλάχιστον) κόσμος είχε κι από ένα κινητό τηλέφωνο στην τσέπη.

Θυμάσαι πως ήταν τα κινητά το 2007, ε; Τότε ακριβώς ήταν που ο Στιβ Τζομπς χάκαρε την έννοια του κινητού, φέρνοντας στην αγορά το iPhone και αλλάζοντας την ιστορία της επικοινωνίας. Ξέρεις τι έκανε στην τελική ο Τζομπς; Εφάρμοσε επακριβώς τον 5ο κώδικα των χάκερς: Δημιούργησε αληθινή τέχνη και ομορφιά με το iPhone.

Η κουλτούρα του χάκινγκ εξαπλώνεται και ανοίγει δρόμους. Διαρκώς διοργανώνονται παντού εκδηλώσεις και δημιουργικές συναντήσεις που ονομάζονται Hackathons, Hackdays ή Hackfests και πραγματοποιούνται σε hackerspaces ή makerspaces ή fablabs ή οπουδήποτε αλλού και θέλουν και κάνουν τους συμμετέχοντες να πειραματιστούν, να γίνουν εφευρετικοί και να ξεπεράσουν τα όρια του δυνατού.

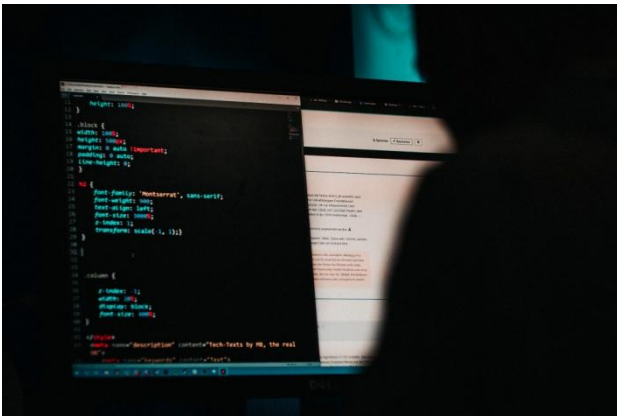


Photo by [Mika Baumeister](#)

Αυτό ακριβώς σου προτείνω να κάνεις κι εσύ. Να ξεφύγεις από τις μανιέρες και τις πεπατημένες, να χακάρεις τη δουλειά σου, να πειράξεις τους κανόνες, να αλλάξεις τον

τρόπο που συμβαίνουν τα πράγματα και να τα κάνεις διαφορετικά, να τα κάνεις καλύτερα. Μην επηρεάζεσαι από τον τρόπο που δουλεύουν οι σημαντικοί και οι διάσημοι στο αντικείμενό σου. Αποδόμησε τις συνταγές επιτυχίας, πάρε τα υλικά και πειραματίσου σε μια νέα συνταγή. Εκμεταλλεύσου τις νέες δυνατότητες που δίνει η τεχνολογία, μελέτησέ τις και δοκίμασε να τις εφαρμόσεις στη δουλειά σου. Μόνο μέσα από το δημιουργικό χάκινγκ θα χαράξεις τα νέα μονοπάτια που επιθυμείς.

Ο Στιούαρτ Μπραντ ήταν μια επιδραστική προσωπικότητα της δεκαετίας του '60, καθώς ήταν εκδότης του περιφημου περιοδικού Whole Earth Catalog.

Το 1972 έγραψε: «Οι χάκερ δεν είναι απλά κάποιοι τεχνικοί. Πρόκειται για μια νέα, κινούμενη ελίτ, με τον δικό της εξοπλισμό, τη δική της γλώσσα, χαρακτήρα και χιούμορ, τους δικούς της μύθους. Αυτοί οι υπέροχοι άνθρωποι με τις ιπτάμενες μηχανές τους χαρτογραφούν τις εσχατιές της τεχνολογίας, μιας παράξενα ανάλαφρης και απαλής τεχνολογίας».

\* Απόσπασμα από το βιβλίο του Γιάννη Φαρσάρη: [“ΣΟΥΣΑΜΙ ΑΝΟΙΞΕ” – Τριάντα τρόποι για να απελευθερώσεις τη δημιουργικότητά σου](#), Εκδόσεις Έσσοππρον, 2022

## ✓ Απομακρυσμένη Ηλεκτρονική Ψηφοφορία

Αναβιώνοντας την «Εκκλησία του Δήμου» στον 21ο αιώνα

// Γράφει ο Χάρης Β. Γεωργίου



Photo by [Parker Johnson](#)



Η ψηφιακή τεχνολογία και οι δυνατότητες των σύγχρονων τηλεπικοινωνιακών δικτύων συχνά δίνουν μια νέα οπτική σε μερικά από τα σημαντικότερα ζητήματα των σύγχρονων κοινωνιών. Μπορεί η «συμμετοχική Δημοκρατία» της Εκκλησίας του Δήμου στην αρχαία Αθήνα να αποτελεί σήμερα ουτοπία στις σύγχρονες πόλεις των πολλών εκατομμυρίων κατοίκων, όμως ο εκμηδενισμός των αποστάσεων μέσω του διαδικτύου και η ευρεία διαθεσιμότητα κρυπτο-γραφικών μεθόδων εξαιρετικά υψηλής αξιοπιστίας και ασφάλειας καθιστούν σήμερα τις διαδικασίες αυτές τεχνικά εφικτές. Αν η τεχνολογία μπορεί να προσφέρει τα μέσα για τη ριζική αναμόρφωση του τρόπου οργάνωσης και διεξαγωγής των πλέον σημαντικών ζητημάτων στις σύγχρονες κοινωνίες, όπως είναι η εκλογή εκπροσώπων και η ίδια η διακυβέρνηση σε μια χώρα, τότε σίγουρα θα αξίζει τα ζητήματα αυτά να τεθούν στη σωστή τους βάση και με τις κατάλληλες προδιαγραφές για το μέλλον.

#### **Η ψηφοφορία ως διαδικασία**

Ένα από τα βασικά συστατικά μιας Δημοκρατίας αποτελεί η ελεύθερη έκφραση της βούλησης των πολιτών μέσα από εκλογικές διαδικασίες για την επιλογή των εκπροσώπων που επωμίζονται τη διακυβέρνηση μιας χώρας. Για να είναι αξιόπιστες και αποτελεσματικές, οι διαδικασίες αυτές πρέπει να βασίζονται σε συγκεκριμένους κανόνες, συνταγματικά κατοχυρωμένους και εφαρμόσιμους στην πράξη, αλλά κυρίως στην έννοια της εμπιστοσύνης. Οι ψηφοφόροι πρέπει να εμπιστεύονται, όχι μόνο τους υποψηφίους που υποστηρίζουν και που θέλουν να επιλέξουν με την ψήφο τους, αλλά και την ίδια τη διαδικασία εκλογής τους, το *δικαίο* του συστήματος – διαφορετικά το τελικό αποτέλεσμα δεν θα μπορέσει να λάβει ουσιαστική *νομιμοποίηση* στο εκλογικό σώμα. Συνεπώς μία παράμετρος μείζονος σημασίας σε οποιοδήποτε εκλογικό σύστημα, ηλεκτρονικό ή μη, είναι η έννοια της *εμπιστοσύνης* σε αυτό, με την έννοια του αδιάβλητου της λειτουργίας και της ακεραιότητάς του.

Παραδοσιακά, μια τυπική εκλογική διαδικασία περιλαμβάνει δύο βασικές ομάδες συμμετεχόντων, τους ψηφοφόρους και τους υποψηφίους, οι οποίες λόγω της αρχής της ελεύθερης συμμετοχής στα κοινά και της ανάδειξης εκπροσώπων (όταν φυσικά αυτό υφίσταται ως αρχή) επικαλύπτονται σε κάποιο ποσοστό. Ένας ψηφοφόρος μπορεί γενικά να είναι και υποψήφιος, συνεπώς πρέπει κάποιος τρίτος, «ουδέτερος», να αναλάβει το διαδικαστικό μέρος της διαδικασίας, ώστε αυτή να παραμείνει αξιόπιστη και αδιάβλητη σε κάθε περίπτωση. Το ρόλο αυτό αναλαμβάνει η *εφορευτική επιτροπή* που απαρτίζεται από (συνήθως τυχαία επιλεγμένα) μέλη του εκλογικού σώματος αλλά όχι υποψηφίων προς εκλογή. Έτσι, η τρίτη αυτή ομάδα αναλαμβάνει το ρόλο του «φύλακα» της ακεραιότητας της εκλογικής διαδικασίας, διασφαλίζοντας μεταξύ άλλων ότι ο κάθε ψηφοφόρος ψηφίζει μόνο μία φορά, ότι ψηφίζουν μόνο όσοι και όπου έχουν δικαίωμα (τόπος, υποψηφίους), ότι στην κάληπ δεν εισάγονται πλαστές ψήφοι, ότι στο τέλος προσμε-

τρούνται όλες σωστά (μόνο οι έγκυρες, μία φορά), κτλ.

Στην παραπάνω τυπική διαδικασία η απαραίτητη υποδομή για την πραγματοποίηση της ψηφοφορίας περιλαμβάνει μια σειρά από μηχανισμούς και μέσα (υλικό) που είναι απαραίτητα για τη διασφάλιση των απαιτούμενων προδιαγραφών. Για παράδειγμα, η μορφή και ο τρόπος συμπλήρωσης των ψηφοδελτίων είναι σαφέστατα καθορισμένα, η κάλπη στην οποία συλλέγονται είναι επίσης συγκεκριμένων προδιαγραφών (κλειδωμένη, συνήθως διαφανής), κάθε συμπληρωμένο ψηφοδέλτιο πρέπει να τοποθετείται σε κλειστό σφραγισμένο φάκελο μέχρι την τελική καταμέτρηση, ενώ τα ψηφοδέλτια διατηρούνται και δεν καταστρέφονται για ένα συγκεκριμένο (σχετικά μεγάλο) χρονικό διάστημα μετά το πέρας της διαδικασίας.

Οι παραπάνω προδιαγραφές δεν είναι καθόλου τυχαίες. Αντίθετα, έχουν προκύψει ως μια πρακτική υλοποίηση κάποιων πολύ βασικών και απαραίτητων κανόνων για μια αξιόπιστη εκλογική διαδικασία οποιασδήποτε μορφής. Αν και οι ακριβείς κανόνες και προδιαγραφές καθορίζονται κάθε φορά από διαφορετικούς παράγοντες, μια αξιόπιστη και ελεύθερη εκλογική διαδικασία πρέπει να χαρακτηρίζεται με βάση τους εξής δέκα κύριους παράγοντες:

1. **Καθολικότητα:** Οποιοσδήποτε πολίτης έχει κατοχυρωμένο δικαίωμα ψήφου, θα πρέπει να μπορεί να συμμετάσχει στη διαδικασία χωρίς κανένα πρόβλημα ή δυσκολία.

2. **Μοναδικότητα:** Κάθε ψήφος προσμετρείται, ακριβώς μία φορά, και αντιστοιχεί

σε ακριβώς έναν ψηφοφόρο (αντιστοιχία 1-προς-1).

3. **Μυστικότητα-Ανωνυμία:** Όταν και όπου απαιτείται, εφαρμόζεται μυστική ή/και ανώνυμη ψηφοφορία.

4. **Ακρίβεια:** Η καταμέτρηση γίνεται σωστά (επισημαίνοντας άκυρα, λευκά, κτλ), επικυρώνεται με δεύτερη (τουλάχιστον) καταμέτρηση και είναι δυνατή και επιπλέον καταμέτρηση αργότερα αν απαιτείται.

5. **Δικαιοσύνη:** Κανείς δεν πληροφορείται επιλεκτικά για τα αποτελέσματα νωρίτερα από άλλους, ειδικά κατά τη διάρκεια διεξαγωγής της ψηφοφορίας.

6. **Διαφάνεια:** Κάθε μηχανισμός, υλικό και αποτέλεσμα είναι δυνατό να ελεγχθεί πριν, κατά τη διάρκεια και μετά το πέρας της διαδικασίας.

7. **Ανθεκτικότητα:** Κανένα επιμέρους λάθος ή παράλειψη, εσκεμμένο ή όχι, δεν πρέπει να είναι καταστροφικό για την εκλογική διαδικασία (πρέπει να υπάρχουν εναλλακτικές λύσεις).

8. **Μη Εξαναγκασμός:** Πρέπει να προστατεύεται η ελευθερία της έκφρασης των ψηφοφόρων ως προς το τι θα επιλέξουν στην κάλπη.

9. **Επιβεβαιωσιμότητα:** Κάθε ψηφοφόρος πρέπει να είναι σε θέση (ο ίδιος) να επιβεβαιώσει ότι η ψήφος του καταχωρήθηκε και καταμετρήθηκε σωστά.

10. **Μη Λογοδοσία:** Στην επιβεβαιωσιμότητα θα πρέπει να προστατεύεται η μυστικότητα της ψήφου (μη αποκάλυψη περιεχομένου).

Οι παραπάνω δέκα παράγοντες αποτελούν ουσιαστικά μια λίστα κριτηρίων βάσει των οποίων μια εκλογική διαδικασία μπορεί να χαρακτηριστεί ως ελεύθερη και δημοκρατική ή όχι. Σε αυτούς τους

παράγοντες προστίθενται φυσικά και μερικοί ακόμα, περισσότερο συνταγματικής φύσης, όπως για παράδειγμα το αν μπορεί να θέσει υποψηφιότητα οποιοσδήποτε από το εκλογικό σώμα, το πώς και από ποιον γίνεται η ταυτοποίηση των στοιχείων κάθε ψηφοφόρου πριν ψηφίσει, κτλ. Επιπλέον, κάποιιοι από τους παραπάνω παράγοντες σε μικρό ή μεγάλο βαθμό αλληλεπικαλύπτονται. Για παράδειγμα, η έννοια της *μυστικότητας* και της *ανωνυμίας* της κάθε ψήφου μοιάζουν ταυτόσημες έννοιες, όμως στην πράξη αφορούν σε διαφορετικά στάδια της εκλογικής διαδικασίας (κατά τη διάρκεια ή μετά την ψηφοφορία, αντίστοιχα).

Σήμερα μια τυπική διαδικασία ψηφοφορίας σε μεγάλη κλίμακα, όπως για παράδειγμα σε κάποιο εθνικό δημοψήφισμα ή σε εθνικές βουλευτικές εκλογές, καλύπτει αρκετές από τις παραπάνω απαιτήσεις αλλά σπανίως το σύνολό τους. Η πιο συνηθισμένη μορφή τέτοιας εκλογικής διαδικασίας περιλαμβάνει τυπωμένα ψηφοδέλτια συγκεκριμένης μορφής, σφραγισμένους (από την εφορευτική επιτροπή) φακέλους στους οποίους τοποθετούνται και συγκεκριμένες τοποθεσίες (εκλογικά κέντρα) όπου πραγματοποιείται η ψηφοφορία. Το πρότυπο αυτό καλύπτει κατά κύριο λόγο τους παράγοντες 1-6 και σε μεγάλο βαθμό και το 7 (*ανθεκτικότητα*) με την προσθήκη εναλλακτικών, έστω και αναχρονιστικών, διαδικασιών σε περίπτωση εμφάνισης κάποιου προβλήματος, όπως για παράδειγμα στη μετάδοση των αποτελεσμάτων κατά την κατάμετρηση. Οι παράγοντες 8-10 αποτελούν εγγενές πρόβλημα όλων ουσιαστικά των τύπων και μεθόδων ψηφοφορίας, καθώς θεωρητικά δεν μπορούν ποτέ να διασφαλιστούν πλήρως.



**Συχνά οι εκλογικές διαδικασίες πρέπει να βασιστούν σε ελάχιστα διαθέσιμα μέσα και να υλοποιηθούν με τον απλούστερο και φθηνότερο τρόπο, χωρίς φυσικά να παραβιαστεί η αξιοπιστία και η εγκυρότητα. Σε χώρες με τεράστιο πληθυσμό ή/και ελάχιστη υποδομή, όπως η Ινδία και το Αφγανιστάν, η ταυτοποίηση των ψηφοφόρων γίνεται μέσω οποιουδήποτε επίσημου εγγράφου (αντί εκλογικού βιβλιαρίου ή μόνο ταυτότητας), ενώ η διασφάλιση της μοναδικότητας της ψήφου εφαρμόζεται το βάψιμο ενός συγκεκριμένου κάθε φορά δακτύλου με ειδικό μελάνι.**

Στην περίπτωση που επιτρέπεται ψηφοφορία εξ' αποστάσεως, αυτό κατά κανόνα πραγματοποιείται με τη μορφή *επιστολικής* ψήφου: η ταυτοποίηση του ψηφοφόρου και η άσκηση του εκλογικού δικαιώματος πραγματοποιείται από κάποια αρμόδια (πιστοποιημένη) αρχή, όπως για παράδειγμα στην αντίστοιχη πρεσβεία σε κάποια άλλη χώρα, ενώ το ψηφοδέλτιο τοποθετείται και πάλι σε σφραγισμένο φάκελο και αποστέλλεται προς καταμέτρηση, κατά κανόνα νωρίτερα από τη διεξαγωγή της κανονικής (τοπικής) ψηφοφορίας. Παρότι ως διαδικασία δεν φαίνεται να διαφέρει σημαντικά, εντούτοις σε πρακτικό-τεχνικό επίπεδο δημιουργούνται νέες απαιτήσεις και προδιαγραφές, οι τρεις πιο σημαντικές εκ των οποίων είναι η πιστοποίηση



κάποιας εναλλακτικής αρχής από την κεντρική, η ασφαλής (μυστικότητα, ακεραιότητα) μεταφορά των ψήφων προς καταμέτρηση και ο ασύγχρονος (όχι ταυτόχρονος) χαρακτήρας της ψηφοφορίας σε αυτή την περίπτωση.

Πώς, όμως, συνδέονται τα παραπάνω με την έννοια της ηλεκτρονικής ψηφοφορίας (e-Voting) και ειδικά της απομακρυσμένης ηλεκτρονικής ψηφοφορίας (Remote e-Voting); Έχει η σύγχρονη τεχνολογία να προσφέρει κάτι στη βελτίωση των παραπάνω διαδικασιών σε ότι αφορά την ποιότητα μιας τυπικής εκλογικής διαδικασίας;

### **Ηλεκτρονική και από απόσταση ηλεκτρονική ψηφοφορία**

Μια πρώτη διάκριση που πρέπει να γίνει είναι μεταξύ των δύο αυτών εννοιών, της απλής ηλεκτρονικής (e-Voting) και της εξ' αποστάσεως ηλεκτρονικής ψηφοφορίας (Remote e-Voting). Η πρώτη αναφέρεται σε εκλογικές διαδικασίες που βασίζονται εν μέρει ή εξ' ολοκλήρου σε τεχνικό επίπεδο σε ηλεκτρονικά μέσα. Για παράδειγμα, τα ψηφοδέλτια μπορεί να είναι τυπωμένα αλλά η συμπλήρωσή τους να γίνεται με τέτοιο τρόπο ώστε να επιτρέπει την καταμέτρησή τους μέσω Η/Υ – εναλλακτικά μπορεί και το ίδιο το «ψηφοδέλτιο» να έχει ηλεκτρονική μορφή στην οθόνη ενός Η/Υ και όλη η διαδικασία να γίνεται με ηλεκτρονικό τρόπο. Παρόμοιες διαδικασίες εφαρμόζονται εδώ και πολλά χρόνια σε χώρες με μεγάλο εκλογικό σώμα (όπως στις ΗΠΑ), όπου η γρήγορη και έγκυρη καταμέτρηση είναι ζήτημα μείζονος σημασίας για την εκλογική διαδικασία. Συνήθως τα συστήματα αυτού του τύπου επιτρέπουν την εφαρμογή κρυπτογραφικών μεθόδων κατάλληλων για την

κάλυψη επιπρόσθετων απαιτήσεων, όπως για παράδειγμα κάποιο ανώνυμο αποδεικτικό «κουπόνι» το οποίο παραλαμβάνει ο ψηφοφόρος και που μπορεί να χρησιμοποιηθεί αργότερα αν χρειαστεί για να επιβεβαιωθεί (διατηρώντας την μυστικότητα της ψήφου του) ότι η επιλογή του καταμετρήθηκε σωστά και συμπεριελήφθη στα συγκεντρωτικά αποτελέσματα.

Η έννοια της «απομακρυσμένης» ηλεκτρονικής ψηφοφορίας προσομοιάζει περισσότερο τη διαδικασία της επιστολικής ψήφου: η εκλογική διαδικασία όχι μόνο περιλαμβάνει ένα ή περισσότερα στάδια «αυτοματοποίησης» μέσω κατάλληλων ηλεκτρονικών διατάξεων αλλά ένας Η/Υ καθίσταται ο ίδιος αρχή πιστοποίησης, εκλογικό κέντρο και μεταφορέας της ψήφου, για κάθε μεμονωμένο ψηφοφόρο, χρησιμοποιώντας τα παγκόσμια τηλεπικοινωνιακά δίκτυα. Οι βασικές προδιαγραφές και οι απαιτήσεις παραμένων οι ίδιες, όμως σε αυτή την περίπτωση κάποιες από αυτές καθίστανται αρκετά δυσκολότερο να ικανοποιηθούν με αξιόπιστο τρόπο και επαρκές επίπεδο. Ενώ σε μια τυπική ψηφοφορία, ηλεκτρονική ή μη, η εκλογική διαδικασία είναι απόλυτα ελεγχόμενη και η εγκυρότητά της διασφαλίζεται σε φυσικό επίπεδο από την εφορευτική επιτροπή και την αρμόδια αρχή, στην απομακρυσμένη ψηφοφορία αυτή η δυνατότητα μετατρέπεται σε μείζον ζήτημα ασφάλειας και αξιοπιστίας. Κάθε ψηφοφόρος, ακόμα και αν διαθέτει τον κατάλληλο εξοπλισμό Η/Υ, πρέπει να μπορεί να ψηφίσει το ίδιο ανώνυμα, έγκυρα, ελεύθερα, αλλά και μοναδικά, με ταυτοποίηση και διαφάνεια, όπως ακριβώς σε τυπικές εκλογικές διαδικασίες με τυπωμένα ψηφοδέλτια, εκλογικά κέντρα και σφραγισμένες κάλπες.

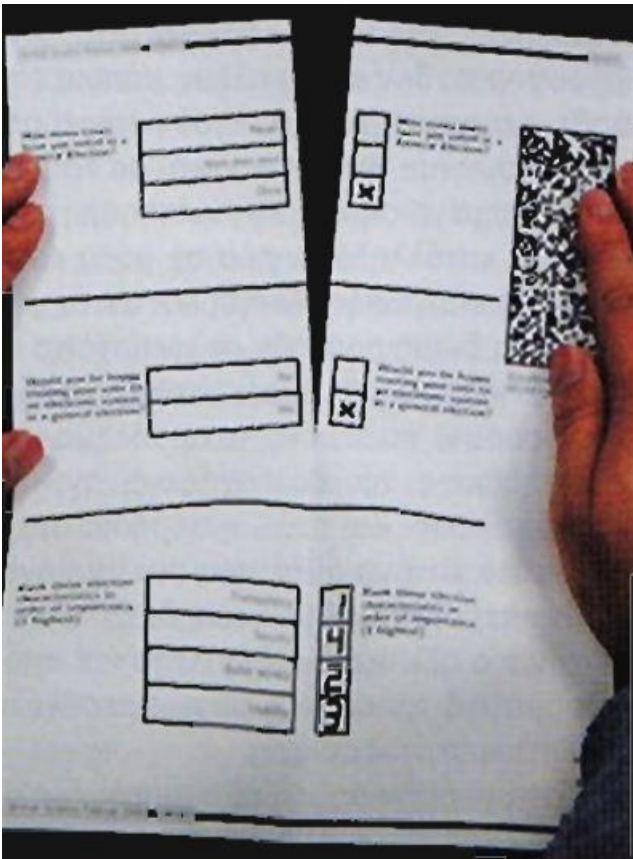
Τα ερωτήματα που προκύπτουν σχετικά με την ηλεκτρονική ψηφοφορία, ειδικά την απομακρυσμένη, είναι αρκετά και δύσκολο να απαντηθούν. Το πρώτο και κύριο ερώτημα φυσικά είναι: Μπορεί η τεχνολογία να διασφαλίσει τουλάχιστον τον ίδιο βαθμό αξιοπιστίας, εγκυρότητας και διαφάνειας με αυτό των παραδοσιακών «φυσικών» τρόπων ψηφοφορίας; Δηλαδή, μπορεί ένα τέτοιο σύστημα να αντικαταστήσει, μερικώς ή καθολικά, μια αντίστοιχη τυπική διαδικασία ψηφοφορίας όπως για παράδειγμα σε εθνικές δημοτικές ή βου-λευτικές εκλογές; Αν η απάντηση στο παραπάνω ερώτημα είναι θετική, το επόμενο λογικό ερώτημα που προκύπτει είναι κατά πόσο κάτι τέτοιο είναι σκόπιμο και θεμιτό, δηλαδή αν και ποια πλεονεκτήματα προσφέρει μια τέτοια επιλογή, πάντα με γνώμονα τη βελτίωση της ίδιας της διαδικασίας (όχι απλά να γίνει μέσω Η/Υ, ως «πείραμα»).

Όπως σε κάθε άλλη δραστηριότητα, έτσι και εδώ, η εφαρμογή των νέων τεχνολογικών εξελίξεων σε ήδη τυποποιημένες διαδικασίες επιλύει κάποια προβλήματα, χωρίς όμως να αποφύγει να δημιουργήσει κάποια νέα. Αν αυτά τα νέα ζητήματα μπορούν να αντιμετωπιστούν με αποτελεσματικό και πρακτικό τρόπο, καθώς και με χαμηλό κόστος, τότε οι νέες αυτές λύσεις ενσωματώνονται επιτυχώς στις διαδικασίες και αποτελούν το νέο πρότυπο.

Το ζήτημα της ηλεκτρονικής ψηφοφορίας αποτελεί ουσιαστικά μια εξαιρετικά θετική εξέλιξη σε ότι αφορά την ακεραιότητα και την ταχύτητα επεξεργασίας των δεδομένων που παράγονται από μια τυπική εκλογική διαδικασία. Αν είναι δυνατό να αυτόματοποιηθεί η διαδικασία ψηφοφορίας από το πρώτο στάδιο, δηλαδή αυτό της συλλογής των ψήφων, τότε όλα τα επόμενα στάδια μπορούν να

επιταχυνθούν σε εξαιρετικά υψηλό επίπεδο, καθώς οι Η/Υ είναι κατασκευασμένοι ακριβώς για τη γρήγορη και σωστή επεξεργασία δεδομένων. Επιπλέον, η ψηφιοποίηση των δεδομένων αυτών στο πρώτο στάδιο επιτρέπει, όπως αναφέρθηκε παραπάνω, την υλοποίηση πρόσθετων μηχανισμών που μέχρι σήμερα δεν υπήρχαν. Για παράδειγμα, σε κάποιες πολιτείες των ΗΠΑ εφαρμόζεται η τεχνική των «τμηματοποιημένων κουπονιών» (splitted e-Ballots), όπου ο ψηφοφόρος χρησιμοποιεί ένα (πιστοποιημένο) ηλεκτρονικό μηχάνημα για να σημειώσει την ψήφο του και εκτυπώνει το αντίστοιχο συμπληρωμένο ψηφοδέλτιο, το οποίο αποτελείται από ένα κωδικό ανωνυμίας (anonymity ID) και δύο ή περισσότερα τμήματα. Ο ψηφοφόρος επιλέγει ένα τμήμα (split) για να ρίξει στην κάλπη και ένα να κρατήσει ο ίδιος ως αποδεικτικό – το ψηφοδέλτιο στην κάλπη έχει ήδη σήμανση γνησιότητας αλλά ταυτόχρονα κανείς άλλος παρά μόνο ο ίδιος μπορεί να διασταυρώσει πλήρως τις καταχωρημένες επιλογές με κάποιο συγκεκριμένο ψηφοφόρο. Παρόμοιες μέθοδοι, όχι απαραίτητα ηλεκτρονικές, ονομάζονται «επιβεβαιώσιμη ψηφοφορία» (verifiable voting).

Στην απομακρυσμένη ηλεκτρονική ψηφοφορία τίθεται επιπλέον το ζήτημα της ασφαλούς (εμπιστευτικής) και έγκυρης (μη τροποποιήσιμης) μετάδοσης της ψήφου μέσω ενός δικτύου Η/Υ, καθώς επίσης και της ταυτοποίησης της ίδιας της ταυτότητας του ψηφοφόρου. Σήμερα τα ζητήματα αυτά μπορούν να επιλυθούν σε πρακτικό επίπεδο μέσω ειδικών κρυπτογραφικών μεθόδων και ασφαλών πρωτοκόλλων επικοινωνίας, τόσο σε επίπεδο ταυτοποίησης όσο και σε επίπεδο κρυπτασφάλειας.



Ένας από τους απλούστερους τρόπους «επιβεβαιώσιμης ψηφοφορίας» (verifiable voting) είναι αυτή όπου ο κάθε ψηφοφόρος μπορεί να ελέγξει, αν χρειαστεί, ότι οι επιλογές του καταχωρήθηκαν και καταμετρήθηκαν κανονικά. Το ψηφοδέλτιο αποτελείται από δύο μέρη (splits) εκ των οποίων το ένα περιλαμβάνει τις διαθέσιμες επιλογές και το άλλο αυτές που επιλέγει ο ψηφοφόρος. Και τα δύο μέρη σημειώνονται με τον ίδιο μοναδικό κωδικό, αλλά χωρίς περισσότερα στοιχεία ταυτοποίησης, και μάλιστα με τρόπο που είναι εύκολο να εντοπιστεί αργότερα (audit trail). Το απαντητικό δελτίο δεν φανερώνει τίποτα για την ταυτότητα του ψηφοφόρου και ταυτόχρονα ο ψηφοφόρος, αν χρειαστεί, μπορεί να αντιπαραβάλλει το πρώτο μισό, το οποίο κρατά ως απόδειξη, και να διαπιστώσει ότι η ψήφος του βρίσκεται χωρίς καμία αλλοίωση στο σύστημα προς καταμέτρηση..

### Πόσο αξιόπιστη είναι μια (απομακρυσμένη) ηλεκτρονική ψηφοφορία;

Μια διαδικασία ψηφοφορίας δεν είναι τίποτα άλλο παρά ένα τυπικό σύστημα μετάδοσης και επεξεργασίας δεδομένων, με κάποιες συγκεκριμένες προδιαγραφές ασφάλειας και αξιοπιστίας. Σε οποιοδήποτε τέτοιο σύστημα το ενδιαφέρον εστιάζεται σε τρεις κύριους παράγοντες: (α) τον αποστολέα του μηνύματος, (β) τον παραλήπτη του μηνύματος και (γ) το κανάλι/μέσο μετάδοσης. Σε μια τυπική «φυσική» ψηφοφορία τα τρία αυτά μέρη «συγχωνεύονται» σε ένα σημείο, απόλυτα ελεγχόμενο, που δεν είναι άλλο από το κάθε εκλογικό κέντρο. Πρακτικά, η διαχείριση της διαδικασίας τόσο κατά τη διάρκεια της ψηφοφορίας όσο και κατά την καταμέτρηση μπορεί να ελεγχθεί απόλυτα και μάλιστα τοπικά. Φυσικά απαιτούνται αντίστοιχες προβλέψεις σε ότι αφορά τη μετάδοση των επιμέρους αποτελεσμάτων για τα γενικά αποτελέσματα και την προσωρινή αποθήκευση των καταμετρημένων ψηφοδελτίων, αλλά και πάλι αυτά είναι ζητήματα που διασφαλίζονται σχετικά εύκολα από την αρμόδια αρχή. Στην περίπτωση της επιστολικής ψήφου η «τοπικότητα» της ψηφοφορίας δεν ισχύει πλέον: κάποια ψηφοδέλτια πρέπει να συλλεγούν και να μεταφερθούν (σε φυσικό επίπεδο) σε κάποιο πιστοποιημένο σημείο καταμέτρησης από κάποιο κατάλληλο φορέα σε ρόλο εφορευτικής επιτροπής. Ακόμα και αν τα ψηφοδέλτια διαμοιραστούν σε αντίστοιχα (π.χ. βάσει καταγωγής των ψηφοφόρων) εκλογικά κέντρα, παραμένει το πρόβλημα της ταυτοποίησης, της συλλογής και της μεταφοράς τους. Και πάλι, η αρμόδια αρχή είναι κατά κανόνα αυτή που αναλαμβάνει τη διεκπεραίωση αυτών των διαδικασιών με τον πιο αξιόπιστο, αδιάβλητο



και αποτελεσματικό τρόπο (π.χ. μέσω πρεσβειών και διπλωματικών σάκων).

Στην περίπτωση της ηλεκτρονικής ψηφοφορίας τα πράγματα είναι αρκετά διαφορετικά. Η διαχείριση ψηφοδελτίων δεν αφορά πλέον φυσικά εκτυπωμένα κουπόνια, τα οποία μπορούν να σφραγιστούν και να υπογραφούν, αλλά ψηφιακά δεδομένα χωρίς ιδιαίτερα εγγενή «φυσικά» χαρακτηριστικά, ενώ ταυτόχρονα μπορούν να αντιγραφούν και να μεταδοθούν πολύ εύκολα. Οι ίδιες οι έννοιες της ταυτοποίησης και της γνησιότητας δεν βασίζονται πλέον στα φυσικά χαρακτηριστικά π.χ. μιας υπογραφής, αλλά σε κρυπτογραφικές μεθόδους και ειδικούς αλγορίθμους ελέγχου πρόσβασης και ακεραιότητας σε επίπεδο ψηφιακών δεδομένων. Πρακτικά, οι ηλεκτρονικές αυτές διαδικασίες διαφέρουν ελάχιστα από τον τρόπο που λειτουργούν οι ηλεκτρονικές συναλλαγές σε εμπορικό επίπεδο: ο κάτοχος μιας πιστωτικής ή χρεωστικής κάρτας, αφού ταυτοποιηθούν τα στοιχεία του ως νόμιμος κάτοχός της, μπορεί να τη χρησιμοποιήσει για να «χρεώσει» ψηφιακά τον τραπεζικό του λογαριασμό σε μια αγορά που κάνει. Προχωρώντας ένα βήμα παραπέρα, η ίδια πιστωτική κάρτα μπορεί να χρησιμοποιηθεί, με κατάλληλες διαδικασίες πιστοποίησης και ασφαλούς μετάδοσης των δεδομένων, σε μια ηλεκτρονική αγορά μέσω διαδικτύου. Στην περίπτωση αυτή η ταυτοποίηση δεν γίνεται μέσω φυσικών χαρακτηριστικών (π.χ. σύγκριση αστυνομικής ταυτότητας με στοιχεία κάρτας και οπτική αναγνώριση ως προς τη φωτογραφία) αλλά μέσω ειδικών κωδικών πρόσβασης και ψηφιακών κρυπτογραφικών πιστοποιητικών που αντικαθιστούν την απλή φυσική υπογραφή του «κατόχου».

Εξετάζοντας τη λίστα που αναφέρθηκε προηγούμενα με τα επιθυμητά χαρακτηριστικά μιας αξιόπιστης και ελεύθερης εκλογικής διαδικασίας (βλ. παράγοντες 1-10), θα πρέπει κανείς να αναλύσει πως μπορεί να υλοποιηθεί κάθε ένας από τους παράγοντες αυτούς σε τεχνικό επίπεδο, μέσω της σύγχρονης ψηφιακής τεχνολογίας, των Η/Υ και των τηλεπικοινωνιακών δικτύων που είναι διαθέσιμα σήμερα. Θεωρώντας ότι κάθε ψηφοφόρος μπορεί να κατέχει ήδη ή να προμηθευτεί προσωρινό ψηφιακό πιστοποιητικό από κάποια αρμόδια αρχή, αντίστοιχης αξιοπιστίας και χρησιμότητας με την αστυνομική ταυτότητα ή το εκλογικό βιβλιάριο, οι απαιτήσεις σχετικά με την ταυτοποίηση του εκάστοτε ψηφοφόρου (καθολικότητα, μοναδικότητα, κτλ) μπορούν να ικανοποιηθούν. Επιπλέον, λόγω της ψηφιακής επεξεργασίας των δεδομένων, η αξιοπιστία σε επίπεδο μεμονωμένων ψήφων (ακρίβεια, μυστικότητα, ανωνυμία, κτλ) είναι σχετικά εύκολο να επιτευχθεί με τη χρήση κατάλληλων κρυπτογραφικών μεθόδων και πρωτοκόλλων μετάδοσης. Σε ότι αφορά κάποιες ειδικές απαιτήσεις που σε μια τυπική «φυσική» ψηφοφορία δεν είναι δυνατό να υλοποιηθούν, στο πλαίσιο της ηλεκτρονικής ψηφοφορίας μπορούν να ενσωματωθούν διαδικασίες επικύρωσης της κάθε ψήφου όχι μόνο από τον ίδιο τον ψηφοφόρο (ηλεκτρονική «απόδειξη» - e-Receipt) αλλά και από την εφορευτική επιτροπή (ηλεκτρονικό «ίχνος» - audit trail) σε όλα τα επίπεδα.

Υπάρχουν, όμως, και κάποια χαρακτηριστικά που ακόμα και στην ηλεκτρονική ψηφοφορία εξακολουθούν να αποτελούν σημαντικό ζήτημα, ίσως μάλιστα σε σοβαρότερο βαθμό. Σε ότι αφορά τον μη εξαναγκασμό και τη μη λογοδοσία,

η μυστικότητα της εκλογικής διαδικασίας (όταν υπάρχει) μέσω ενός παραβάν και ενός κλειστού σφραγισμένου φακέλου όπου τοποθετείται το συμπληρωμένο (ανώνυμο) ψηφοδέλτιο θεωρείται ως επαρκής μηχανισμός, τουλάχιστον σε ότι αφορά το άμεσο τοπικό περιβάλλον της διεξαγωγής της ψηφοφορίας αλλά και της μη ιχνηλασιμότητας του κάθε ψηφοφόρου. Στην ηλεκτρονική ψηφοφορία η μυστικότητα φαίνεται να ενισχύεται, όμως ο τρόπος δημιουργίας και χρήσης των αντίστοιχων ψηφιακών πιστοποιητικών καθιστά τα ζητήματα της ανωνυμίας και της μη ιχνηλασιμότητας αρκετά δυσκολότερο να ικανοποιηθούν. Συγκεκριμένα, εκτός από την εφορευτική επιτροπή, είναι απαραίτητη πλέον μια πρόσθετη αρμόδια αρχή, αυτή της προσθήκης ενός σταδίου ανωνυμίας (anonymizer), η οποία αποσυνδέει την ταυτότητα/γνησιότητα της ψηφιακής ψήφου (e-Ballot) από τη διαδικασία συμπλήρωσης του αντίστοιχου δελτίου και άρα του ψηφοφόρου-χρήστη του συστήματος. Με άλλα λόγια, επειδή λόγω της διαδικασίας που υλοποιούν τα πρωτόκολλα ασφαλείας η ταυτότητα του χρήστη πρέπει να επικυρώνεται τη στιγμή που συμπληρώνει το κάθε μεμονωμένο (πλέον) ψηφοδέλτιο, αυτό θα πρέπει με κάποιο τρόπο να διατηρεί την εγκυρότητά του αλλά να χάνει την προέλευσή του. Έτσι, ο κάθε πιστοποιημένος ψηφοφόρος συνήθως προμηθεύεται (μετά την ταυτοποίησή του) από την αρχή αυτή ένα μοναδικό ηλεκτρονικό «κουπόνι» μιας χρήσης (e-Token), το οποίο μεταδίδεται χωρίς άλλα στοιχεία στην εφορευτική επιτροπή και που χρησιμοποιεί ως μηχανισμό πιστοποίησης της ψήφου αλλά όχι του ίδιου. Ο λόγος που η αρχή έκδοσης αυτών των ηλεκτρονικών κουπονιών μιας χρήσης πρέπει να είναι διαφορετική από την εφορευτική επιτροπή που

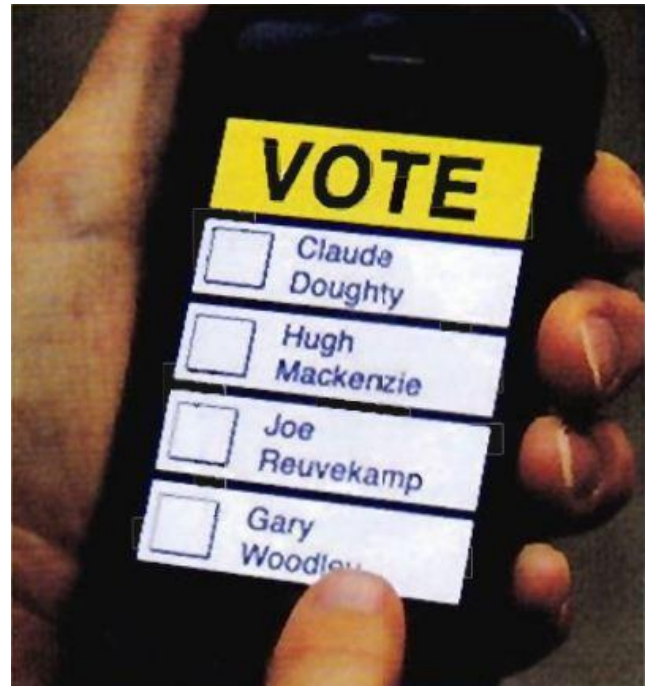
διαχειρίζεται τις ψήφους είναι ακριβώς για να μην μπορεί κανένα από τα δύο αυτά μέρη να έχει πλήρη ταυτοποίηση ψηφοφόρων-ψηφών, χωρίς όμως να υποβαθμίζεται η αξιοπιστία του συστήματος.



**Οι ηλεκτρονικές συσκευές άμεσης καταχώρησης ψήφων (Direct-Recording Electronic – DRE voting machines) αποτελούν σήμερα την πιο συνηθισμένη μορφή ηλεκτρονικής ψηφοφορίας. Κατά κανόνα δεν υλοποιούν μια αμιγώς εξ' αποστάσεως αλλά απλά μια αποκεντρωμένη διαδικασία ηλεκτρονικής ψηφοφορίας, η οποία διεξάγεται με τυπικό τρόπο σε εκλογικά κέντρα. Η διαφορά έγκειται στο ότι μέσω των συσκευών αυτών η αδιαβλητότητα του συστήματος βασίζεται κυρίως σε κρυπτογραφικές μεθόδους, άρα απαιτούν πολύ πιο περιορισμένη υποδομή, και επιπλέον η καταχώρηση και καταμέτρηση γίνεται σχεδόν σε πραγματικό χρόνο.**

Αν και παρόμοιοι μηχανισμοί ενισχύουν σε μεγάλο βαθμό τη δυνατότητα επιβεβαίωσης από την πλευρά του ψηφοφόρου, άρα και την εμπιστοσύνη του στο σύστημα και στη διαδικασία, εντούτοις η δυνατότητα πλήρους αποσύνδεσης του ψηφοφόρου από την «τοπικότητα» του εκλογικού κέντρου καθιστά, σύμφωνα με αρκετούς μηχανικούς Πληροφορικής αλλά και πολιτικούς αναλυτές, σημαντικά αυξημένο τον κίνδυνο έναντι της απαίτησης για μη εξαναγκασμό και μη λογοδοσία. Εφόσον η ψηφοφορία δεν διεξάγεται πλέον

σε περιορισμένο, απόλυτα ελεγχόμενο φυσικό χώρο (εκλογικό κέντρο), υπάρχει σαφέστατος κίνδυνος σχετικά με το αν ο ψηφοφόρος εκφράζεται ελεύθερα ή/και αν το αποδεικτικό που θα λάβει, αν είναι πλήρες ως προς το περιεχόμενο του ψηφοδέλιου (όχι απλά κωδικός επιβεβαίωσης), δεν ενισχύει τον κίνδυνο εξαγοράς ψήφων. Πρακτικά, υπάρχει πραγματικό και εξαιρετικά πολύπλοκο δίλημμα μεταξύ της εφαρμογής κρυπτογραφικών μεθόδων για τη διασφάλιση της εμπιστευτικότητας και ταυτόχρονα της ανάγκης διατήρησης της ανωνυμίας, ακριβώς λόγω της ίδιας της φύσης των τεχνικών λύσεων που υφίστανται σήμερα. Κάποιοι μάλιστα ισχυρίζονται ότι οι δυσκολίες αυτές είναι τέτοιες που «...ποτέ ένα ηλεκτρονικό σύστημα ψηφοφορίας δεν μπορεί να είναι αρκούντως ασφαλές», ειδικότερα όταν τα αντίστοιχα συστήματα υλικού (hardware) και λογισμικού (software) που χρησιμοποιούνται είναι απλά «πιστοποιημένα» αλλά όχι πλήρως βασισμένα σε ανοικτά πρότυπα (open standards). Η αλήθεια βρίσκεται μάλλον κάπου μεταξύ των δύο ακραίων περιπτώσεων. Σίγουρα κανένα ηλεκτρονικό σύστημα δεν μπορεί να ικανοποιήσει πλήρως όλες τις απαιτήσεις ασφάλειας, αξιοπιστίας, ακεραιότητας, κτλ. Από την άλλη πλευρά, κανένα παραδοσιακό σύστημα ψηφοφορίας, με τυπωμένα ψηφοδέλτια, κανονικά εκλογικά κέντρα και σφραγίδες μελανιού δεν είναι περισσότερο ασφαλές ή αξιόπιστο εν γένει, καθώς τα προβλήματα είναι μεν διαφορετικά αλλά το ίδιο σημαντικά.



**Η σύγχρονη τεχνολογία και η εξέλιξη των φορητών συσκευών επιτρέπει πλέον την υλοποίηση συστημάτων ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ακόμα και με τη χρήση «έξυπνων» τηλεφώνων από οπουδήποτε, ακόμα και σε περιοχές με πολύ περιορισμένη σταθερή (ενσύρματη) τηλεπικοινωνιακή υποδομή.**

### **Ηλεκτρονικά συστήματα ψηφοφορίας και κρυπτασφάλεια**

Ένας από τους πιο σημαντικούς παράγοντες στη σχεδίαση και την υλοποίηση των συστημάτων ηλεκτρονικής ψηφοφορίας (e-Voting), ειδικά όταν πρόκειται για εξ' αποστάσεως (remotely), αποτελεί η ασφάλεια. Ειδικότερα, σε παρόμοια συστήματα το ενδιαφέρον επικεντρώνεται και στους τρεις βασικούς άξονες ενός τηλεπικοινωνιακού μοντέλου, δηλαδή τον πομπό (ψηφοφόρος), τον παραλήπτη (κάλπη) και το μέσο μετάδοσης. Ως προς το τελευταίο, όταν πρόκειται για απομακρυσμένη ψηφοφορία μέσω διαδικτύου, υπάρχει σαφέστατη ανάγκη για αδιαβλητότητα, ακεραιότητα, αλλά και μυστικότητα-ανωνυμία της κάθε ψήφου. Στο



πλαίσιο αυτό, εφόσον πρόκειται για μη ελεγχόμενα δίκτυα εξαιρετικά μεγάλης έκτασης και χωρίς καμία διασφάλιση εμπιστευτικότητας, η μοναδική μέθοδος διασφάλισης των παραπάνω απαιτήσεων είναι μέσω κατάλληλων κρυπτογραφικών μεθόδων.

Πρακτικά, αυτό που απαιτείται είναι ένα σύστημα το οποίο να προσφέρει (α) αξιόπιστη πιστοποίηση του κάθε μέρους στα άκρα του καναλιού επικοινωνίας και (β) προστασία των μηνυμάτων που ανταλλάσσονται τόσο σε επίπεδο ακεραιότητας (να μην μπορούν να τροποποιηθούν από τρίτο) όσο και σε επίπεδο εμπιστευτικότητας (προστασία μυστικότητας). Τα θέματα αυτά εν γένει δεν είναι καθόλου απλά – ειδικότερα το ζήτημα της απόλυτα ασφαλούς ανταλλαγής του κλειδιού σε ένα τυπικό μοντέλο ανταλλαγής κρυπτογραφημένων μηνυμάτων αποτελεί ένα θεωρητικά άλυτο μαθηματικό πρόβλημα. Παρόλα αυτά, εδώ και μερικές δεκαετίες οι δυνατότητες των Η/Υ επιτρέπουν την υλοποίηση μεθόδων που επιλύουν το πρόβλημα αυτό με «πρακτικά επαρκή» τρόπο.

Υπάρχουν δύο κατηγορίες κρυπτογραφικών συστημάτων: (α) τα *συμμετρικά*, όπου τα δύο μέρη που επικοινωνούν χρησιμοποιούν ένα κοινό προ-συμφωνημένο κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων τους, και (β) τα *ασύμμετρα*, όπου κάθε μέρος χρησιμοποιεί ένα ζευγάρι κλειδιών που περιλαμβάνει ένα κλειδί μόνο για κρυπτογράφηση («δημόσιο») και ένα μόνο για αποκρυπτογράφηση («ιδιωτικό»). Το πλεονέκτημα της δεύτερης αυτής κατηγορίας κρυπτοσυστημάτων είναι ο διαχωρισμός των δύο ενεργειών – εφόσον η κρυπτογράφηση γίνεται με «ασύμμετρο» (όχι απλά ταυτόσημα αντίστροφο) τρόπο, το ίδιο συμβαίνει και με τα δύο μέρη του ζευγαριού των κλειδιών. Στην πράξη, είναι σαν να κατασκευάζεται

μία πόρτα η οποία κλειδώνει μόνο με το πρώτο «δημόσιο» κλειδί και ξεκλειδώνει μόνο με το δεύτερο «ιδιωτικό» κλειδί. Έτσι, αν τα δύο κλειδιά είναι «αρκούντως ασύνδετα» μεταξύ τους, δηλαδή η γνώση το ενός δεν υποδηλώνει τίποτα για το άλλο, η διαρροή του πρώτου κλειδιού δεν συνιστά κανέναν κίνδυνο και συνεπώς μπορεί να μεταδοθεί ελεύθερα χωρίς κανένα πρόβλημα.

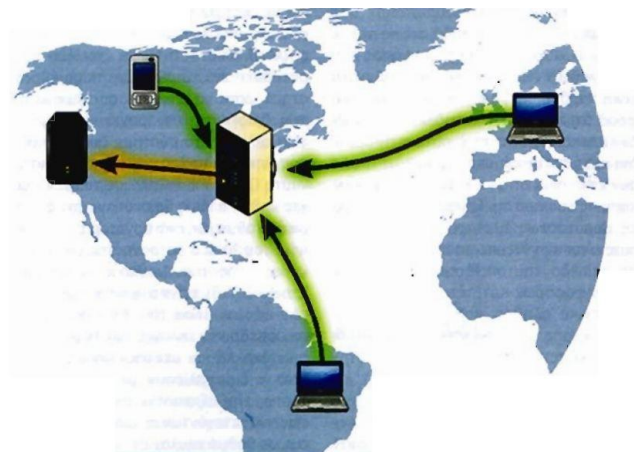
Το 1977 οι Ron Rivest, Adi Shamir και Leonard Adleman του MIT δημοσίευσαν μια ιστορική πλέον εργασία τους ακριβώς για την επίλυση του παραπάνω προβλήματος, αυτό της δημιουργίας ενός (τυχαίου) ζευγαριού κλειδιών με τα παραπάνω χαρακτηριστικά, δηλαδή να είναι «συμπληρωματικά» ως προς την κρυπτογράφηση-αποκρυπτογράφηση, να μην μπορεί να τα «μαντέψει» κάποιος εύκολα και επιπλέον να είναι τέτοια ώστε η γνώση του ενός να μην υποβαθμίζει τη μυστικότητα του άλλου κλειδιού. Ο αλγόριθμος RSA, όπως τον ονόμασαν με τα αρχικά των ονομάτων τους, βασίστηκε στην εγγενή δυσκολία της παραγοντοποίησης πολύ μεγάλων ακεραίων αριθμών σε πρώτους παράγοντες και επιπλέον στους πάρα πολλούς συνδυασμούς που προκύπτουν για την ομαδοποίηση των παραγόντων αυτών σε δύο «ομάδες». Χρησιμοποιώντας μαθηματικές μεθόδους και θεωρήματα από τη Θεωρία Αριθμών, κατάφεραν να αποδείξουν ότι η κάθε τέτοια (εν γένει τυχαία) ομάδα πρώτων παραγόντων μπορεί να δημιουργήσει ένα από τα δύο κλειδιά του ζευγαριού και μάλιστα βάσει του περίφημου «Κινέζικου θεωρήματος των υπολοίπων» είναι δυνατό να υλοποιηθούν με αποδοτικό τρόπο οι αντίστοιχες διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης μηνυμάτων. Σχεδόν ταυτόσημο αλγόριθμο είχε διατυπώσει νωρίτερα το

1973 ο βρετανός μαθηματικός Clifford Cocks, σε διαβαθμισμένο όμως έγγραφο, το οποίο δεν δημοσιεύτηκε παρά μόλις το 1997.

Η ασφάλεια ενός τέτοιου συστήματος βασίζεται στο γεγονός ότι αν το γινόμενο των δύο ομάδων πρώτων αριθμών είναι «αρκούντως μεγάλο» και η ακριβής σύστασή τους είναι «αρκούντως τυχαία», πρακτικά είναι αδύνατο από το πρώτο (δημόσια διαθέσιμο) κλειδί κρυπτογράφησης και μια σειρά κρυπτογραφημένων μηνυμάτων να μαντέψει κάποιος το δεύτερο (μυστικό) κλειδί αποκρυπτογράφησης. Η έννοια «αρκούντως τυχαία» αφορά στο πως ακριβώς διαμοιράζονται οι πρώτοι παράγοντες του αρχικού γινομένου στις δύο ομάδες, ενώ το «αρκούντως μεγάλο» ως προς το μέγεθος των κλειδιών εξαρτάται από τις εκάστοτε τεχνικές δυνατότητες των Η/Υ που πιθανόν να αναλάβουν το έργο της κρυπτανάλυσης. Με βάση τις σημερινές προβλέψεις για τις επόμενες γενιές Η/Υ και με βάση τις σημερινές μαθηματικές μας γνώσεις (αν δεν υπάρχει κάποιο θεώρημα ευκολότερης παραγοντοποίησης που δεν έχει ανακαλυφθεί ακόμη), ένα ζευγάρι κλειδιών τύπου RSA με μέγεθος τουλάχιστον 2048 bits ( $2^{2048} \approx 3,16 \times 10^{616}$  συνδυασμοί) είναι ασφαλές από επιθέσεις κρυπτανάλυσης τύπου «brute force attacks» για πολλές χιλιάδες χρόνια.

Εκτός από τη βασική διατύπωση του αλγορίθμου RSA, παρόμοιες τεχνικές έχουν διατυπωθεί για αντίστοιχα ή ισοδύναμα ασύμμετρα κρυπτοσυστήματα, όπου ένα ζευγάρι κλειδιών «τύπου RSA» κατασκευάζεται βάσει ενός εξαιρετικά δύσκολου μαθηματικού (συνήθως συνδυαστικού) προβλήματος και στη συνέχεια τα δύο κλειδιά χρησιμοποιούνται ως συμπληρωματικά για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Οι

τεχνικές αυτές αποτέλεσαν πραγματική επανάσταση στα ψηφιακά δίκτυα τηλεπικοινωνιών και ιδιαίτερα στα πρώτα στάδια του διαδικτύου τις δεκαετίες του '70 και του '80, καθώς κατέστησαν δυνατή την ασφαλή μετάδοση πληροφοριών χωρίς την ανάγκη κανενός άλλου πρόσθετου μέσου μετάδοσης κλειδιών και πιστοποιητικών ασφαλείας. Κατά κανόνα οι ασύμμετρες μέθοδοι κρυπτογράφησης όπως ο RSA είναι πολύ πιο απαιτητικές και αργές σε σύγκριση με τις περισσότερες συμμετρικές μεθόδους (κοινού μοναδικού κλειδιού) που προσφέρουν ανάλογο επίπεδο ασφάλειας. Έτσι, η ασύμμετρη κρυπτογράφηση συνήθως εφαρμόζεται στο πρώτο στάδιο της επικοινωνίας, όπου το «δημόσιο» κλειδί κάθε μέρους μεταδίδεται ελεύθερα και μέσω αυτού κρυπτογραφείται ένα νέο, μυστικό κλειδί από κοινού χρήσης, και σε δεύτερο στάδιο η κύρια επικοινωνία διεξάγεται με συμμετρική κρυπτογράφηση, καθώς ήδη έχει εξασφαλιστεί η ασφαλής «συμφωνία» ενός τυχαίου κλειδιού για αυτό το σκοπό. Η διαδικασία αυτή αποτελεί εδώ και αρκετές δεκαετίες το βασικό μοντέλο ασφαλούς επικοινωνίας στο διαδίκτυο και εφαρμόζεται με διάφορες παραλλαγές και υλοποιήσεις σε όλες σχεδόν τις περιπτώσεις όπου απαιτείται υψηλό επίπεδο ασφάλειας στη μετάδοση μηνυμάτων (πρωτόκολλα SSL/TLS για ηλεκτρονική τραπεζική, ηλεκτρονικές αγορές, ιδιωτικά δίκτυα τύπου VPN, κ.ά.).



Η χρήση εξελιγμένων κρυπτογραφικών μεθόδων όπως οι αλγόριθμοι ασύμμετρης κρυπτασφάλειας τύπου RSA καθιστούν δυνατή τη δημιουργία «εικονικών» ιδιωτικών δικτύων υψηλού επιπέδου ασφάλειας (Virtual Private Network – VPN), ακόμα και διαμέσου ενός εντελώς «ανοικτού» δικτύου διαμεσολάβησης όπως είναι το Internet. Στην περίπτωση ηλεκτρονικής ψηφοφορίας εξ' αποστάσεως, παρόμοια δίκτυα εγκαθιδρύονται είτε μόνιμα, μεταξύ εκλογικών κέντρων και αρμόδιας αρχής, είτε ακόμα και προσωρινά, με σκοπό τη διασύνδεση ενός μεμονωμένο ψηφοφόρου με κάποιο εικονικό εκλογικό κέντρο για την καταχώρηση της ψήφου του/της.

Είναι φανερό πως οι παραπάνω έννοιες, ιδιαίτερα αυτή ενός «δημόσιου» κλειδιού που μπορεί να μεταδοθεί ελεύθερα και που συνδέεται εγγενώς με ένα άλλο «ιδιωτικό» κλειδί, συνδέονται άμεσα με τις απαιτήσεις ασφάλειας σε ένα σύστημα ηλεκτρονικής εξ' αποστάσεως ψηφοφορίας. Αλγόριθμοι όπως ο RSA διασφαλίζουν ότι κάθε μέρος της διαδικασίας, τόσο ο εκάστοτε ψηφοφόρος όσο και η διοργανώτρια αρχή (ως ηλεκτρονική «κάλπη»), μπορεί να κατασκευάσει ένα μοναδικό, τυχαίο ζευγάρι κλειδιών, να δημοσιοποιήσει ένα εκ των δύο και τελικά να εγκαθιδρύσει έναν ασφαλή δίαυλο επικοινωνίας τύπου σημείο-προς-σημείο (point-to-point), μέσω του οποίου μπορεί με αξιό-

πιστο και ασφαλή τρόπο να καταχωρήσει την ψήφο του. Ένα εξίσου σημαντικό, όμως, πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων τύπου RSA είναι το γεγονός ότι, εν γένει, τα δύο κλειδιά μπορούν να χρησιμοποιηθούν και με «αντίστροφη» σειρά (καθώς είναι συμπληρωματικά) αν κάτι τέτοιο απαιτείται. Με άλλα λόγια, η έννοια του «δημόσιου» και του «ιδιωτικού» κλειδιού μπορεί να αντιστραφεί, αν κάτι πρέπει να μπορεί να κρυπτογραφηθεί μοναδικά από τον κάτοχο του μυστικού κλειδιού και να μπορεί να αποκρυπτογραφηθεί από οποιονδήποτε βάσει του δημόσια διαθέσιμου αντίστοιχου κλειδιού. Ίσως αυτό να μοιάζει κάπως αντιφατικό, όμως αποτελεί τη βάση της έννοιας της ψηφιακής υπογραφής και του ψηφιακού πιστοποιητικού: αν κάτι μπορεί να «σημανθεί» με μοναδικό τρόπο από κάποιον και στη συνέχεια να «ελεγχθεί» από οποιονδήποτε άλλο, αυτή ακριβώς η διαδικασία έχει την έννοια της υπογραφής, με ψηφιακό όμως τρόπο, η ασφάλεια της οποίας βασίζεται εξ' ολοκλήρου σε κρυπτογραφικούς αντί για βιομετρικούς παράγοντες (γραφικός χαρακτήρας).

Αν κάτι μπορεί να «υπογραφεί» ψηφιακά μόνο από τον κάτοχο του «ιδιωτικού» κλειδιού και στη συνέχεια να μεταδοθεί ελεύθερα ως «γνήσιο», με τη δυνατότητα ελέγχου του οποιαδήποτε στιγμή μέσω του αντίστοιχου «δημόσιου» κλειδιού, ένα τέτοιο ασύμμετρο κρυπτοσύστημα τύπου RSA ικανοποιεί επιπλέον και την απαίτηση της πιστοποίησης σε μια ηλεκτρονική εξ' αποστάσεως ψηφοφορία. Έτσι, για την ταυτοποίηση του κάθε ψηφοφόρου εξ' αποστάσεως το μόνο που χρειάζεται είναι το διαθέσιμο «δημόσιο» κλειδί του να φέρει την ψηφιακή υπογραφή (πιστοποίηση εγκυρότητας) από την

εκάστοτε αρμόδια ανώτατη αρχή πιστοποίησης-ταυτοποίησης των ψηφοφόρων. Η απαραίτητη υποδομή που απαιτείται για την αποθήκευση και τη διαθεσιμότητα των «δημόσιων» κλειδιών όλων των χρηστών τους συστήματος συνήθως αναφέρεται ως «Υποδομή Δημόσιων Κλειδιών» (Public Key Infrastructure – PKI) και μπορεί να είναι είτε δημόσια είτε ιδιωτική, επίσημα θεσμοθετημένη ή ανεπίσημη ως ένα απλό συνεργατικό δίκτυο (π.χ. η ελεύθερα προσβάσιμη υπηρεσία PKI του MIT).

Αξίζει επιπλέον να σημειωθεί ότι η αρμόδια αρχή πιστοποίησης έχει πρόσβαση μόνο στο «δημόσιο» κλειδί κάποιου προς πιστοποίηση χρήστη του συστήματος – το «ιδιωτικό» κλειδί δημιουργείται και παραμένει πάντοτε μυστικό και γνωστό μόνο στον κάτοχό του. Πρακτικά, η έννοια της πιστοποίησης ενός ψηφοφόρου στις τυπικές (μη ηλεκτρονικές) διαδικασίες ψηφοφορίας περιλαμβάνει αντίστοιχο «δημόσιο κλειδί», δηλαδή βιομετρικά και μη βιομετρικά χαρακτηριστικά του ατόμου που (ειδικά τα πρώτα) είναι αρκετά δύσκολο να αντιγραφούν και να χρησιμοποιηθούν από τρίτο, καθώς και «υπογραφή» (πιστοποίηση εγκυρότητας-αξιοπιστίας) από την αρμόδια αρχή, δηλαδή ειδικό χαρτί, σήμανση, σφραγίδες, κτλ. Ο τρόπος που λειτουργούν τα ψηφιακά πιστοποιητικά είναι παρόμοιος, με τη βασική όμως διαφορά ότι το αντίστοιχο «ιδιωτικό» κλειδί δεν αποκαλύπτεται ποτέ, ούτε στην αρμόδια αρχή πιστοποίησης, καθώς κάτι τέτοιο δεν είναι απαραίτητο. Έτσι, θα μπορούσε κάποιος να υποστηρίξει πως ένα σύστημα ηλεκτρονικής εξ' αποστάσεως ψηφοφορίας είναι εν γένει περισσότερο ασφαλές σε επίπεδο ταυτοποίησης-πιστοποίησης των ψηφοφόρων. Κάτι τέτοιο όμως δεν είναι γενικά αληθές, καθώς η αξιοπιστία της έγκυρης ταυτοποίησης του

ψηφοφόρου έγκειται αποκλειστικά και μόνο στην ασφαλή αποθήκευση (μη διαρροή) και χρήση (όχι από τρίτους) του αντίστοιχου «ιδιωτικού» κλειδιού, που άλλωστε ως ψηφιακό δεδομένο μπορεί εύκολα να αντιγραφεί και να μεταδοθεί αν δεν έχει προστατευθεί σωστά σε τεχνικό επίπεδο. Το γεγονός αυτό καταδεικνύει πόσο η ψηφιακή Παιδεία αποτελεί ίσως τον πιο καθοριστικό παράγοντα σε συστήματα ηλεκτρονικής ψηφοφορίας, εξίσου ή περισσότερο σημαντικό από το επίπεδο ασφάλειας του ίδιου του συστήματος σε καθαρά τεχνικό επίπεδο.



Η πλειοψηφία των πρωτοκόλλων επικοινωνίας στο διαδίκτυο σήμερα διατηρούν τη μορφή «βασισμένη σε κείμενο» (plaintext format) για τη μεταφορά δεδομένων, κυρίως για λόγους συμβατότητας με παλαιότερα συστήματα. Ακόμα και έτσι, με τη χρήση κατάλληλων κρυπτογραφικών πρωτοκόλλων, τα περιεχόμενα των μηνυμάτων διατηρούνται «αναγνώσιμα» ως εκτυπώσιμο κείμενο, όμως τα δεδομένα που μεταφέρουν είναι διασφαλισμένα με τους ισχυρότερους αλγορίθμους κρυπτογράφησης. Στον παγκόσμιο ιστό (World Wide Web – WWW) οι ηλεκτρονικές αγορές ή ηλεκτρονικές τραπεζικές συναλλαγές γίνονται με αυτό τον τρόπο, μέσω ασφαλών πρωτοκόλλων και μηχανισμών (SSL/TLS, πρωτόκολλο «https» αντί «http»).

### Επίλογος

Είναι, λοιπόν, η ηλεκτρονική ψηφοφορία πανάκεια στα προβλήματα της συμμετοχικότητας και της

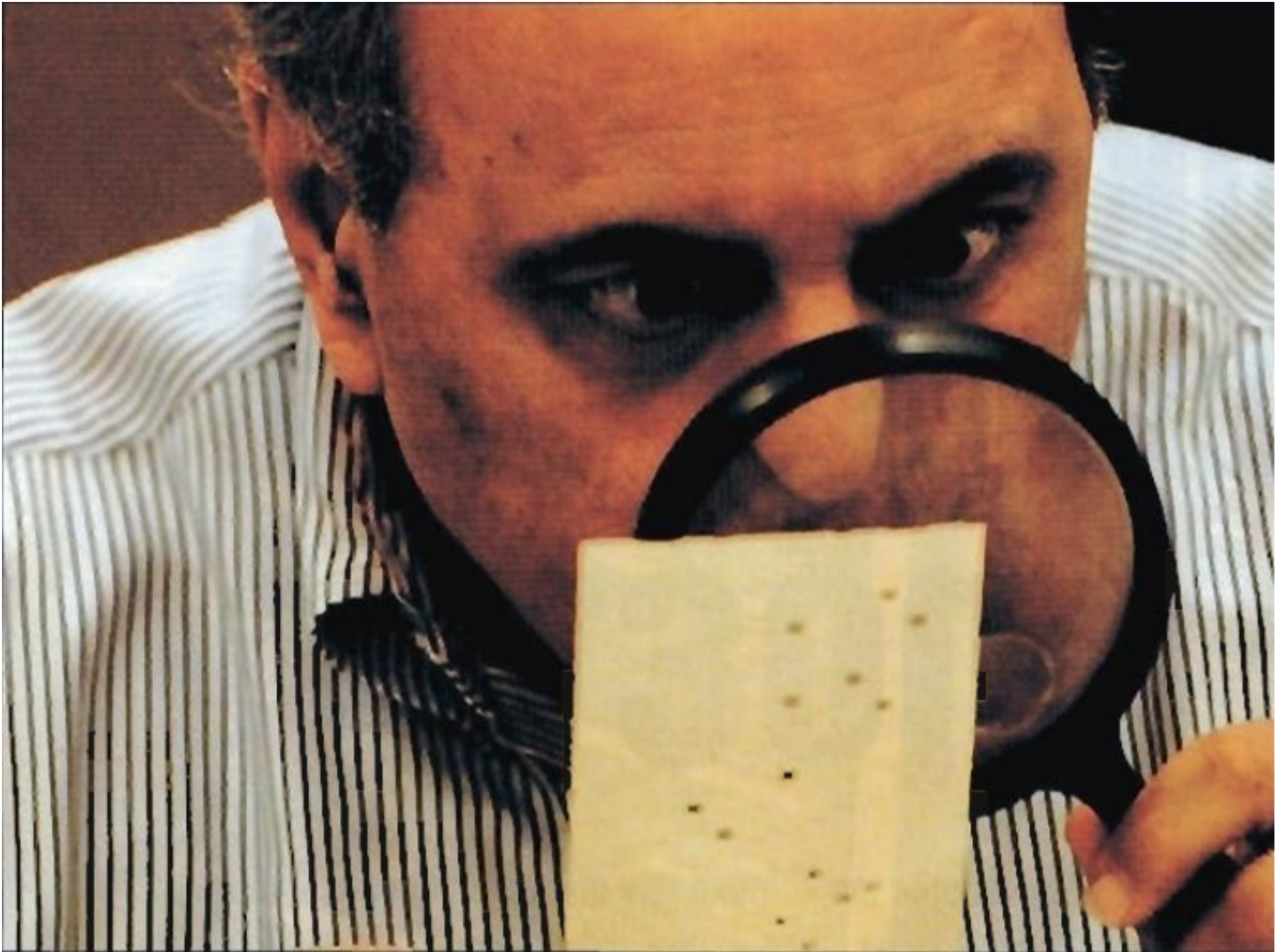


αποτελεσματικής διακυβέρνησης στις σύγχρονες κοινωνίες; Μπορεί η εξ' αποστάσεως ψηφοφορία μέσω διαδικτύου να βελτιώσει την ποιότητα της Δημοκρατίας και του αισθήματος δικαιοσύνης, πολύ περισσότερο και με σαφώς καθοριστικότερο τρόπο από ότι οι λεγόμενες «επαναστάσεις του διαδικτύου» όπως στην Αίγυπτο και στην Τυνησία; Η απάντηση δεν είναι καθόλου εύκολη και απαιτεί μεγάλη προσοχή, καθώς υπάρχει ο κίνδυνος η τεχνολογία να αναβαθμιστεί ως αυτοσκοπός και στον όρο «ηλεκτρονική ψηφοφορία» να δοθεί βάση αποκλειστικά στο πρώτο, παραβλέποντας το δεύτερο (πολύ πιο σημαντικό) συνθετικό.

Από τεχνική άποψη, η δυνατότητα ασφαλούς, αξιόπιστης, ελεύθερης εκλογικής διαδικασίας, με προστασία των ατομικών δικαιωμάτων και του αδιάβλητου του αποτελέσματος, σαφέστατα υπάρχει εδώ και μερικές δεκαετίες. Με τη χρήση κατάλληλων κρυπτογραφικών μεθόδων, το διαδίκτυο μπορεί να μετατραπεί σε ανθεκτικό και αδιάβλητο μέσο ασφαλούς μετάδοσης, κατάλληλο για οποιουδήποτε τύπου εξ' αποστάσεως ηλεκτρονική ψηφοφορία. Μάλιστα η NASA έχει ήδη κατασκευάσει από το 1997 ένα παρόμοιο σύστημα για να μπορούν οι αστροναύτες που βρίσκονται σε τροχιά να ψηφίζουν στις εκλογές – χρησιμοποιήθηκε για πρώτη φορά από τον αστροναύτη David Wolf το 1997 σε τοπικές εκλογές καθώς ο ίδιος βρισκόταν στο διαστημικό σταθμό Mir και αργότερα, το Νοέμβριο του 2004, ο αστροναύτης Leroy Chiao, κυβερνήτης του Διεθνούς Διαστημικού Σταθμού (ISS), έγινε ο πρώτος αμερικανός που ψήφισε μέσω του ίδιου συστήματος σε προεδρικές εκλογές των ΗΠΑ. Ασφαλή πρωτόκολλα και μέθοδοι μπορούν πράγματι να διασφαλίσουν, με κρυπτογραφικό

τρόπο, την αξιοπιστία της πιστοποίησης των συμμετεχόντων σε μια τέτοια διαδικασία, σε βαθμό τουλάχιστον παρόμοιο ή καλύτερο από ότι τα σημερινά «παραδοσιακά» μέσα ταυτοποίησης.

Παρόλα αυτά, είναι εξαιρετικά σημαντικό να μην παραβλέπεται το γεγονός ότι κανένα τεχνολογικό μέσο ή επίτευγμα δεν είναι απόλυτα αξιόπιστο, ούτε απόλυτα προσβάσιμο ή κατανοητό από το σύνολο των ατόμων που εν γένει αφορά. Για τη διεξαγωγή μιας διαδικασίας ψηφοφορίας με τον «παραδοσιακό» τρόπο απαιτούνται κάποια ελάχιστα φυσικά μέσα, όπως για παράδειγμα ψηφοδέλτια, κάλπες, παραβάν (αν πρόκειται για μυστική ψηφοφορία), κτλ, ενώ σε αυτή είναι εφικτό να συμμετάσχει ουσιαστικά το σύνολο του πληθυσμού. Αντίθετα, σε μια ηλεκτρονική εξ' αποστάσεως ψηφοφορία απαιτείται η ύπαρξη Η/Υ και τηλεπικοινωνιακών δικτύων, ηλεκτρικό ρεύμα (όχι αυτονόητο παγκοσμίως) και κυρίως ψηφιακή Παιδεία και *ικανότητα χρήσης* της αντίστοιχης τεχνολογίας από κάθε ψηφοφόρο. Οι περιορισμοί αυτοί είναι καθοριστικοί, μερικές φορές απαγορευτικοί, τόσο σε πρακτικό όσο και σε νομικό-συνταγματικό επίπεδο, βάσει της αρχής της ισονομίας κι της δικαιοσύνης. Για το λόγο αυτό, κυρίως, η απομακρυσμένη ηλεκτρονική ψηφοφορία αποτελεί ακόμα ένα σημαντικό, αλλά συμπληρωματικό, μέσο διεξαγωγής εκλογικών διαδικασιών, ακόμα και στις πιο προηγμένες χώρες του πλανήτη. Άλλωστε, δεν είναι λίγοι αυτοί που υποστηρίζουν την άποψη ότι οι εκλογές ανέκαθεν ήταν και πρέπει να παραμείνουν μια εξόχως «συμμετοχική» διαδικασία, κάτι παραπάνω από την απλή «τεχνική» διαδικασία συλλογής και καταμέτρησης ψήφων, κάθε φορά με τον πιο αποτελεσματικό τρόπο.



Το Νοέμβριο του 2000 στις προεδρικές εκλογές των ΗΠΑ, η πολιτεία της Florida υπήρξε το πρώτο ίσως τόσο σημαντικό παράδειγμα σχετικά με την εγγενή δυσκολία που εμπεριέχει το εγχείρημα της πλήρους αυτοματοποίησης της εκλογικής διαδικασίας με τεχνικά μέσα. Μετά από καταγγελίες για εσφαλμένη καταχώρηση ψήφων και σημαντικότερες αστοχίες στη λειτουργία των μηχανών DRE που χρησιμοποιήθηκαν στα εκλογικά κέντρα, δόθηκε εντολή επανακαταμέτρησης των ψήφων από τους ανθρώπους των εφορευτικών επιτροπών. Σύντομα διαπιστώθηκε ότι οι προδιαγραφές της μηχανογράφησης, κυρίως το μέγεθος και ο τρόπος σήμανσης των δελτίων με τις καταχωρημένες ψήφους, καθιστούσαν το επιχείρημα αυτό εξαιρετικά δύσκολο και αμφίβολο. Μετά από σχεδόν μία εβδομάδα και με καταμετρημένες μόλις 175.037 από συνολικά 6.000.000 περίπου ψήφους, το ανώτατο δικαστήριο έδωσε εντολή να διακοπεί η επανακαταμέτρηση επικυρώνοντας ταυτόχρονα τα αρχικά αποτελέσματα, παρότι ήταν βέβαιο ότι η έκβαση στη συγκεκριμένη πολιτεία ήταν καθοριστική για την εκλογή του επόμενου προέδρου των ΗΠΑ (2000).

[ Πρώτη δημοσίευση ]

[Περιοδικό Περισκόπιο](#), τ. 379, Οκτώβριος 2013

### ✓ Χώρες και ηλεκτρονικά συστήματα ψηφοφορίας

e-Voting	Remote e-Voting	Μελλοντικά πλάνα
Αυστραλία, Βραζιλία, Καναδάς, Γαλλία, Ινδία, Ιαπωνία, Καζακστάν, Περού, Ρωσία, ΗΠΑ, ΗΑΕ, Βενεζουέλα	Αυστρία, Αυστραλία, Καναδάς, Εσθονία, Γαλλία, Ιαπωνία, Ελβετία	Αργεντινή, Αζερμπαϊτζάν, Λευκορωσία, Βουλγαρία, Χιλή, Τσεχία, Φινλανδία, Ελλάδα, Ιταλία, Λετονία, Λιθουανία, Μεξικό, Νεπάλ, Νιγηρία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Σλοβακία, Σλοβενία, Ισπανία, Ν. Αφρική, Ν. Κορέα, Σουηδία

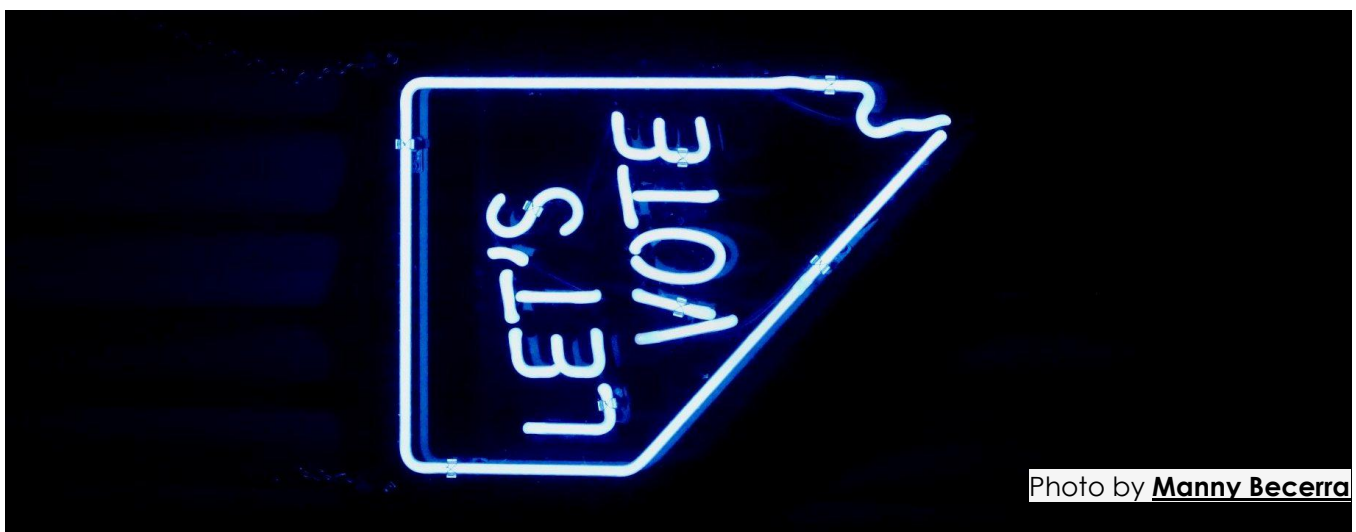
Στον παραπάνω πίνακα παρουσιάζεται συνοπτικά η διείσδυση των τεχνολογιών ηλεκτρονικής ψηφοφορίας ανά χώρα παγκοσμίως. Η πρώτη στήλη (e-Voting) αφορά σε χώρες που ήδη εφαρμόζουν συστήματα ηλεκτρονικής ψηφοφορίας σε επίπεδο καταχώρησης σε τυπικά εκλογικά κέντρα ή «σταθμούς» ηλεκτρονικής ψηφοφορίας (polling stations). Στις περισσότερες περιπτώσεις τα συστήματα αυτά αποτελούνται από ειδικά τερματικά ηλεκτρονικής συμπλήρωσης και εκτύπωσης των συμπληρωμένων ψηφοδελτίων. Αξίζει να σημειωθεί ότι το νομοθετικό πλαίσιο που ισχύει στις ΗΠΑ επιτρέπει διαφορετικές προβλέψεις και προδιαγραφές ανά πολιτεία, με αποτέλεσμα τα αντίστοιχα συστήματα να εμφανίζουν σημαντικότερες διαφοροποιήσεις.

Στη δεύτερη στήλη παρουσιάζονται χώρες που έχουν ήδη υλοποιήσει σε επίπεδο πραγματικών εκλογών (περιφερειακών, κοινοβουλευτικών ή ευρωεκλογών) συστήματα απομακρυσμένης ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου ή μέσω τηλεφώνου. Από τις χώρες αυτές, η Αυστραλία και η Εσθονία είναι ίσως αυτές με τη μεγαλύτερη εμπειρία και τεχνογνωσία, καθώς έχουν εφαρμόσει παρόμοια συστήματα εκτεταμένα εδώ και αρκετά χρόνια. Η Εσθονία αποτελεί ίσως το πιο επιτυχημένο παράδειγμα στην Ευρώπη μαζικής ψηφοφορίας εξ' αποστάσεως σε εθνικό επίπεδο (όχι μόνο αντί επιστολικής ψήφου), καθώς ήδη από το 2002 διαθέτει το κατάλληλο νομοθετικό πλαίσιο και παρά τα προβλήματά του φαίνεται πως το

σύστημα λειτουργεί αρκετά αξιόπιστα, με χρήση «έξυπνων» καρτών (smartcards) και ψηφιακών υπογραφών (digital signatures). Το 2005 έγινε η πρώτη χώρα παγκοσμίως που προσέφερε τη δυνατότητα ηλεκτρονικής ψηφοφορίας μέσω διαδικτύου σε εθνικό επίπεδο (περιφερειακές εκλογές).

Στην τρίτη ομάδα ανήκουν οι χώρες που διαθέτουν συστήματα ηλεκτρονικής ψηφοφορίας υπό δοκιμή, καθώς και χώρες που τώρα σχηματίζουν την αντίστοιχη νομοθεσία και σχεδιάζουν σύντομα να αποκτήσουν παρόμοια συστήματα. Αξίζει να σημειωθεί ότι στην πλειοψηφία τους οι χώρες αυτές χαρακτηρίζονται από το μέγεθος του εκλογικού σώματος ή/και από τη γεωγραφική τους έκταση: είτε είναι πολύ μικρές, οπότε είναι εύκολη η σχεδίαση και η πιλοτική εφαρμογή ηλεκτρονικής ψηφοφορίας, είτε είναι πολύ μεγάλες, οπότε ένα τέτοιο σύστημα διευκολύνει πολύ τη διαδικασία.

Στην Ελλάδα το εκλογικό σώμα είναι της τάξης των 10 εκατομμυρίων πολιτών, με μεγάλο και συνεχώς αυξανόμενο ποσοστό αποχής από την εκλογική διαδικασία (29,1% στις εθνικές εκλογές του 2009). Από αυτούς, η διείσδυση του διαδικτύου ανέρχεται σήμερα περίπου στα 4 εκατομμύρια κατοίκους, με σημαντικές, όμως, αποκλίσεις ως προς το επίπεδο ψηφιακής Παιδείας. Σήμερα η ελληνική νομοθεσία προβλέπει ψήφο επιστολική ή με «άλλο πρόσφορο μέσο» μόνο για τους μόνιμους κατοίκους Ελλάδας. Βάσει των τελευταίων εκλογικών αποτελεσμάτων, το μεγαλύτερο ποσοστό των ψηφοφόρων που δεν ψήφισαν ήταν κυρίως νέοι με μέσο ή ανώτερο επίπεδο γνώσεων σε ότι αφορά τη χρήση νέων τεχνολογιών. Κατά συνέπεια, η υλοποίηση ενός συστήματος απομακρυσμένης ηλεκτρονικής ψηφοφορίας στην Ελλάδα ίσως έχει σημαντικότερα οφέλη σε ότι αφορά το ποσοστό συμμετοχής σε μελλοντικές εκλογικές διαδικασίες.

Photo by **Manny Becerra**



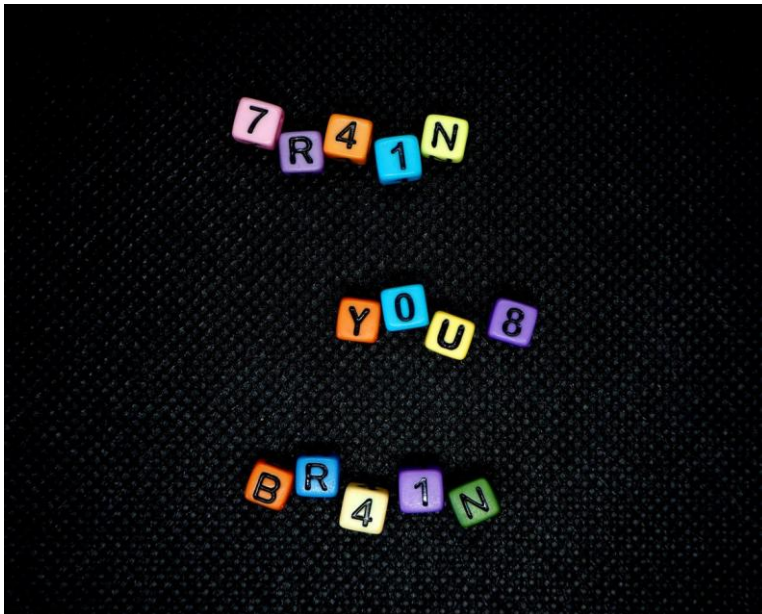


Photo by Margarida Afonso

## ✓ Brain – train

(και ουχι 'drain')

Γρίφοι & προβλήματα από την  
Επιστήμη των Υπολογιστών για μαθητές

// Επιμέλεια: **Φώτης Αλεξιάκος**

### ✓ Εξάσκηση 1

Σε ένα συρτάρι έχετε 21 ζευγάρια κίτρινες και 21 ζευγάρια μαύρες κάλτσες. Χωρίς να βλέπετε, πόσες τουλάχιστον κάλτσες πρέπει να τραβήξετε για να είστε σίγουροι πως έχετε στα χέρια σας τουλάχιστον ένα ζευγάρι όμοιες κάλτσες;

(Αγνώστου)

### ✓ Εξάσκηση 2

2) Πέντε πειρατές βρίσκονται ναυαγοί σε ένα έρημο νησί. Στο νησί ο μόνος κάτοικος είναι ένας πίθηκος και η μοναδική τροφή που υπάρχει είναι καρύδες. Αρχίζουν λοιπόν οι ναυαγοί να μαζεύουν καρύδες σε ένα μεγάλο σωρό. Όταν νύχτωσε όντας πολύ κουρασμένοι πέφτουν για ύπνο με σκοπό να μοιραστούν τις καρύδες εξίσου, το επόμενο πρωί.

Κατά τη διάρκεια της νύχτας ένας πειρατής ξυπνά, σκεπτόμενος ότι οι άλλοι μπορεί να προσπαθήσουν να τον εξαπατήσουν στην μοιρασιά, και αποφασίζει να πάρει το μερίδιο του νωρίτερα, χωρίζει τις καρύδες σε πέντε ισοπληθείς σωρούς και διαπιστώνοντας ότι

περισσεύει μια καρύδα την δίνει στον πίθηκο. Κρύβει έναν απ' τους πέντε σωρούς και τους υπόλοιπους τους κάνει έναν σωρό και πέφτει για ύπνο.

Αργότερα, ο δεύτερος πειρατής ξυπνά με την ίδιες υποψίες ότι οι υπόλοιποι θα τον «ρίξουν» στην μοιρασιά και κάνει το ίδιο πράγμα ,χωρίζει τις καρύδες σε πέντε σωρούς πάλι περισσεύει μια καρύδα την οποία δίνει στον πίθηκο. Στη συνέχεια κρύβει το μερίδιό του, συγκεντρώνει τους υπόλοιπους σωρούς σε ένα έναν μεγαλύτερο και πέφτει για ύπνο.

Ο ένας μετά τον άλλο και οι υπόλοιποι πειρατές κάνουν ακριβώς το ίδιο...

Όταν οι πειρατές ξυπνούν το επόμενο πρωί όλοι παρατήρησαν ότι ο σωρός καρυδών είναι πολύ μικρότερος από ότι ήταν το προηγούμενο βράδυ, αλλά δεδομένου ότι κάθε πειρατής είναι τόσο ένοχος όσο και οι άλλοι, κανείς δεν λέει τίποτα. Τότε χωρίζουν τις καρύδες (για έκτη φορά) σε πέντε ίσα μέρη και παίρνει ο καθένας από ένα.

Ποιος είναι ο **μικρότερος** αριθμός από καρύδες που θα μπορούσαν να υπάρχουν στον αρχικό σωρό ώστε να μπορεί να υλοποιηθεί η παραπάνω διαδικασία;

*(Ben Williams, Saturday Evening Post, 1926).*

### ✓ Εξάσκηση 3

Διαθέτουμε έναν βράχο συνολικής μάζας 121Kgr. Μπορούμε να τον κόψουμε σε όσα κομμάτια **ακέραιας** μάζας θέλουμε. Σκοπεύουμε να τον κόψουμε σε κομμάτια για να τα χρησιμοποιήσουμε ως σταθμά που να ζυγίζουν **οποιαδήποτε ακέραια** ποσότητα ανάμεσα στο 1 και στα 121 κιλά. Ποιος είναι ο ελάχιστος αριθμός κομματιών, στα οποία πρέπει να τον σπάσουμε και πόσα κιλά θα είναι το καθένα; Μπορείτε να γενικεύσετε την λύση;

*(Αγνώστου)*

---

✓ Στείλτε αν θέλετε τις δικές σας λύσεις στο [newsletter@epe.org.gr](mailto:newsletter@epe.org.gr)

★ Οι απαντήσεις των γρίφων θα δημοσιευθούν στο επόμενο τεύχος

## ✓ Brain – train

### Οι λύσεις των γρίφων του προηγούμενου τεύχους

#### Πρόβλημα 1

Το “μυστικό” είναι να εκμεταλλευτούμε την λογική πράξη exclusive OR (XOR:  $\oplus$ ). Όπου:  $\mathbf{x \oplus y = x' y + x y'}$ . Στη γλώσσα C ο σχετικός τελεστής είναι ο  $\wedge$  (caret). Το ζητούμενο υλοποιείται κάπως έτσι:

```
int x,y;

scanf("%d %d", &x, &y);

x=x^y; y=x^y; x=x^y;

printf("%d %d\n",x,y);
```

#### Πρόβλημα 2

Ο αριθμός 1296 προφανώς αναλύεται ως γινόμενο πολλών τριάδων ακεραίων. Αν όλες οι τριάδες είχαν διαφορετικό άθροισμα, ο απογραφέας, ο οποίος προφανώς γνωρίζει τον αριθμό του σπιτιού, θα μπορούσε άμεσα να βρει την τριάδα των ηλικιών χωρίς να χρειαστεί καμιά επιπλέον πληροφορία. Πλην όμως, ζητά το πλήθος των παρκαρισμένων αυτοκινήτων. Άρα έχουμε τουλάχιστον δυο τριάδες των οποίων το άθροισμα είναι ίδιο. Με λίγο *gute force* ψάξιμο, βρίσκουμε μόνο δυο τέτοιες (με το ίδιο άθροισμα όρων δηλαδή). Τις (1,18,72) και (2,8,81). Με άλλα λόγια:  $1+18+72=2+8+81=91$  και αυτός (91) είναι και ο αριθμός του σπιτιού.

### Πρόβλημα 3

Η δυσκολία εδώ είναι πως οι αριθμοί ... παραγίνονται μεγάλοι ακόμα και για τον υπολογιστή. Αν εκμεταλλευτούμε όμως κάποιες ιδιότητες των λογαρίθμων και συγκεκριμένα της συνάρτησης  $\log_{10}()$  τα πράγματα απλουστεύονται αρκετά. Έχουμε λοιπόν:

$$\log_{10}(X!) = \log_{10}(1) + \log_{10}(2) + \log_{10}(3) + \dots + \log_{10}(X)$$

Επίσης, για  $X > 0$  το  $\lfloor \log_{10}(X) \rfloor + 1$  μας δίνει το πλήθος των ψηφίων του ακεραίου  $X$ . Προσθέτοντας το 1 λοιπόν στο 2ο σκέλος της παραπάνω παράστασης, παίρνουμε τον αριθμό των ψηφίων του  $X!$  χωρίς να αναγκαστούμε να υπολογίσουμε πολύ μεγάλους ακεραίους. Έτσι, η υλοποίηση της λύσης (π.χ. σε γλώσσα C) είναι πλέον τετριμμένη.

```
#include <stdio.h>
#include <math.h>

int main(int argc, char *argv[])
{
    long N,X,i,digits=1;
    float fd=0.0;

    printf("N=? ");
    scanf("%ld", &N);
    X=1;i=2;
    while (digits<=N-1)
    {
        while (i<=X)
        {
            fd += log10f((float)i);
            i++;
        }
        digits = (long)floorf(fd);
        if (digits == N-1)
            printf("%ld, X=%ld\n",digits+1,X);
        X++;
    }
    return 0;
}
```





Επισκεφθείτε μας στο web  
[www.epe.org.gr](http://www.epe.org.gr)

**Γίνετε μέλος της ΕΠΕ**

Για την ανάδειξη της  
Πληροφορικής στη χώρα

Η Ένωση Πληροφορικών Ελλάδος υπάρχει για να δημιουργεί τις προϋποθέσεις για την προαγωγή της Πληροφορικής, αξιοποιώντας τις δυνάμεις των Πληροφορικών και ικανοποιώντας τις εργασιακές και επιστημονικές τους ανάγκες όπου και αν εργάζονται ή διαμένουν. Είναι η κατάληξη της αναζήτησης όλων των Πληροφορικών για ένα ισχυρό φορέα του κλάδου που να αναδεικνύει αξιόπιστα τον κοινωνικό τους ρόλο και να τους εκπροσωπεί αυθεντικά σε όλα τα πεδία των ενδιαφερόντων τους.

Είναι η αφετηρία μιας μεγαλόπνοης προσπάθειας που επιδιώκει να κινητοποιήσει όλες τις ζωντανές δυνάμεις της κοινωνίας και να πορευτεί, μαζί μ' αυτές, προς έναν καλύτερο κόσμο για όλους.

Σταθμός σε αυτή την πορεία και στρατηγικός στόχος της ΕΠΕ είναι η δημιουργία του Επιμελητηρίου Πληροφορικής.

Η δράση και οι παρεμβάσεις της είναι ο καταλύτης για την ωρίμανση των αναγκαίων κοινωνικών και πολιτικών συνθηκών.

Οι αξίες που καλλιεργεί θα αποτελέσουν την κληρονομιά και το όραμα του θεσμικού αυτού φορέα. Για να μπορέσουν όλοι οι πληροφορικοί να βρουν τη θέση που τους αξίζει στον κόσμο που όλοι μας οραματιζόμαστε.



<https://www.facebook.com/EnosiPliororikonElladas>



<https://www.linkedin.com/groups?gid=66328>



[https://twitter.com/epe\\_gr](https://twitter.com/epe_gr)



<https://www.youtube.com/user/hiuaccount>



<http://www.epe.org.gr/index.php?id=7&type=100>