Ομιλία 22/10/2007

Αναστασία Φύλλα, Συνάντηση εργασίας ομάδας Ια5 – Ebusiness Forum

Είναι γεγονός ότι η ολοένα και πιο διαδεδομένη ψηφιοποίηση των πληροφοριών έχει επιφέρει και την συνεπακόλουθη μεταβολή των μεθόδων ταυτοποίησης των ατόμων. Από την εποχή της φυσικής ταυτοποίησης κατά την οποία η φυσική και μόνο παρουσία του ατόμου όχι μόνο λειτουργούσε αλλά επαρκούσε για την απόδειξη όλων εκείνων των μοναδικών ιδιοτήτων και χαρακτηριστικών που έφερε μια οντότητα, έχουμε περάσει στην εποχή της ψηφιακής ταυτοποίησης όπου η αποδεικτική ισχύς της φυσικής παρουσίας έχει αντικατασταθεί από την ψηφιακή ταυτότητα του ατόμου.

Είναι σημαντικό να έχει κανείς στο νου ορισμένους φορείς ταυτοποίησης όπως για παράδειγμα το γνωστό σε όλους μας αριθμό Δελτίου Αστυνομικής Ταυτότητας, τον αριθμό του φορολογικού μητρώου, τον αριθμό μητρώου ασφάλισης προκειμένου να κατανοήσει τις δυο πολύ βασικές λειτουργίες που επιτελούν δηλαδή

Α)την μοναδική ταυτοποίηση του ατόμου δηλαδή την διάκριση του από άλλες οντότητες με τις οποίες υπάρχει κατά περίπτωση κίνδυνος σύγχυσης λόγω πιθανής σύμπτωσης ιδιοτήτων ή χαρακτηριστικών

Β)Την παροχή ικανού αριθμού πληροφοριών σε σχέση με τον φορέα των πληροφοριών, οι οποίες μπορούν να λειτουργήσουν ως ένας λεπτομερής απολογισμός της κατά περίπτωση συμπεριφοράς του (για παράδειγμα ο αριθμός φορολογικού μητρώου αποτελεί ένα στοιχείο που δίνει την δυνατότητα στο άτομο που έχει πρόσβαση στα κατάλληλα συστήματα να

λάβει γνώση όλων των πληροφοριών φορολογικού χαρακτήρα του υποκειμένου στο οποίο αναφέρεται).

Το ερώτημα λοιπόν που τίθεται σε εμάς είναι αν η διευρυμένη χρήση των ψηφιακών ταυτοτήτων (η οποία σε κάθε περίπτωση περιλαμβάνει την εμπλοκή και ιδιωτικών φορέων) θα επιτρέψει την ταυτόχρονη ικανοποίηση των συμφερόντων των κυβερνήσεων, των ιδιωτικών φορέων και των πολιτών και ειδικότερα, την νόμιμη κυβερνητική πρόσβαση και διαχείριση των προσωπικών δεδομένων, την αποτελεσματικότητα των διαδικτυακών υπηρεσιών και τέλος το αίτημα για αποτελεσματική προστασία των προσωπικών δεδομένων των πολιτών[1]. Παράλληλα, η μετάβαση στην ολοένα και ευρεία «ψηφιακή διασύνδεση» των οργανωσιακών συστημάτων της δημόσιας σφαίρας ελλοχεύει και κινδύνους που έχουν να κάνουν με την παρεμβατικότητα της δημόσιας διοίκησης στην σφαίρα του αυτοκαθορισμού και της ελευθερίας του πολίτη δίχως να του αφήνει περιθώρια αντίδρασης[2].

Οι νομικοί προβληματισμοί που δημιουργούνται από την παραπάνω κατάσταση εντοπίζονται κυρίως σε 2 βασικά σημεία

Α)Η αποδυνάμωση της διεργασίας ταυτοποίησης του ατόμου μέσω της φυσικής του παρουσίας συνεπάγεται την απώλεια ενός μεγάλου τμήματος πληροφοριών που απαιτούνται κατά τις συναλλαγές και αυταπόδεικτα και παραδοσιακά καλύπτονταν από την φυσική συνάφεια. Το πρόβλημα που ταυτοποίησης που δημιουργείται με την έλλειψη φυσικής συνάφειας θα πρέπει να τονισθεί ότι σε κάθε περίπτωση είναι δυσδιάστατο δηλαδή

[1]Mary Rundle, “International data protection and digital identity management tools”, available at http://cyber.law.harvard.edu/home/uploads/577/Rundle_Identity_Mashup_Background.pdf
[2] Μωραιτάκης Νικόλαος, «Ο ρόλος της ηλεκτρονικής διακυβέρνησης στη δημόσια διοίκηση», Διοικητική Ενημέρωση 2004, σελ. 86

Α)Αναφέρεται τόσο στην επιβεβαίωση ότι μια υπηρεσία παρέχεται και προέρχεται πράγματι από την αρμόδια δημόσια υπηρεσία,

Β) όσο και στο ότι ο πολίτης που κάνει χρήση των δημοσίων ηλεκτρονικών εφαρμογών και συναλλάσσεται με την διοίκηση, είναι πραγματικά αυτός που ισχυρίζεται ότι είναι.

Αυτό το πληροφοριακό κενό δημιούργησε εύλογα ένα κλίμα ανασφάλειας κατά τις συναλλαγές το οποίο κλήθηκε εκ των πραγμάτων να αντιμετωπίσει ο νομοθέτης υιοθετώντας διαδικασίες πιστοποίησης των πληροφοριών. Χαρακτηριστικό παράδειγμα αυτών αποτελεί η υιοθέτηση της νομοθεσίας αναφορικά με τις ψηφιακές υπογραφές, μέσω του π.δ 150/2001[3] το οποίο αποτελεί ενσωμάτωση στην ελληνική έννομη τάξη της Οδηγίας 99/93 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου.

Τα σημεία που αξίζει να σημειώσουμε στο συγκεκριμένο προεδρικό διάταγμα είναι τα ακόλουθα

1. Η εξίσωση των έννομων συνεπειών της ιδιόχειρης υπογραφής στο τομέα του ουσιαστικού και δικονομικού δικαίου με την προηγμένη ηλεκτρονική υπογραφή δηλαδή αυτή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής.

2. Την διάκριση της απλής από την προηγμένη ηλεκτρονική υπογραφή. Το π.δ τονίζει όμως ότι η διάκριση αυτή δεν αίρει την ισχύ και το παραδεκτό της απλής ηλεκτρονικής υπογραφής ως αποδεικτικό μέσο.

[3] ΦΕΚ Α 125/2001

Β)Ο δεύτερος νομικός προβληματισμός που εγείρεται από την ψηφιακή ταυτοποίηση των ατόμων αφορά την διαχείριση των προσωπικών δεδομένων του υποκειμένου που οι πληροφορίες αυτές αφορούν. Το ζήτημα της προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα αντιμετωπίσθηκε νομοθετικά μέσω του νόμου 2472/1997[4] και μιας σειράς αποφάσεων που εκδόθηκαν από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα η οποία είναι αρμόδια για την τήρηση των εν λόγω διατάξεων. Σημειωτέον δε ότι οι διατάξεις του προαναφερθέντος νόμου εφαρμόζονται και στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία[5]. Επικουρικά, και για λόγους πληρότητας θα μπορούσαμε στο σημείο αυτό να αναφέρουμε και το νόμο 3471/2006 ο οποίος αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[6].

Τα σημεία που χρήζουν ιδιαίτερης σημασίας από τον νόμο 2472/1997 και τα οποία σχετίζονται με το ζήτημα της διαχείρισης των ψηφιακών ταυτοτήτων είναι τα ακόλουθα

1. Κάθε άτομο είναι φορέας του συνταγματικά προστατευόμενου δικαιώματος του πληροφοριακού αυτοκαθορισμού[7]. Αυτό σημαίνει ότι δικαιωματικά πρέπει να είναι σε θέση να ελέγχει και να διαχειρίζεται κατά βούληση την διάχυση και επεξεργασία των πληροφοριών που το αφορούν και προσδιορίζουν και οι οποίες αποτελούν σε οποιαδήποτε φάση αντικείμενο επεξεργασίας.

[4] ΦΕΚ Α 50/1997
[5] άρθρο 3 παρ.1 Ν. 2472/1997
[6] ΦΕΚ Α 133/2006
[7] Σ άρθρο 9^{A} «Καθένας έχει δικαίωμα προστασίας από την συλλογή επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί όπως νόμος ορίζει. Σ άρθρο 5^{A}, «Καθένας έχει δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσης τους αποτελεί υποχρέωση του κράτους, τηρουμένων πάντα των εγγυήσεων των άρθρων 9,9^{A}, και 19»

Το δικαίωμα αυτό, αν και δεν μπορούμε να πούμε ότι απόλλυται ολοσχερώς, με βεβαιότητα πλήττεται καθώς η χρήση των τεχνολογιών επιφέρει την αυτόματη δημιουργία ψηφιακών αντιγράφων των δεδομένων που τίθενται υπό επεξεργασία κατά τρόπο τέτοιο ώστε δυσχεραίνεται η δυνατότητα του υποκειμένου των δεδομένων να ελέγξει την διαχείριση τους και να περιορίσει την πρόσβαση τρίτων ατόμων σε αυτά. Η παραδοχή λοιπόν «ότι κανένας δεν είναι ελεύθερος εαν γνωρίζει (ή ακόμη περισσότερο αν υποψιάζεται) ότι παρακολουθείται και ότι η καταγραφή της δράσης του αυτονομείται από το «φυσικό» περιβάλλον της, γίνεται πληροφορία που μπορεί να αποτελέσει αντικείμενο μελέτης και αξιολόγησης της προσωπικότητας του, χωρίς κατοχύρωση της δυνατότητας του για επέμβαση, είναι ένας σημαντικός κίνδυνος που πιθανολογείται στην περίπτωση της διαχείρισης των ψηφιακών ταυτοτήτων κατά την διενέργεια ηλεκτρονικών συναλλαγών με την δημόσια διοίκηση[8].

2. Ιδιαίτερα σημαντικό είναι και το γεγονός ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα από οποιαδήποτε δημόσια αρχή, την καθιστά «υπεύθυνο επεξεργασίας[9]» και εγείρει στο πρόσωπο της τις υποχρεώσεις που ο νόμος απαιτεί για την νόμιμη συλλογή και επεξεργασία αυτών.

Προκειμένου λοιπόν τα δεδομένα προσωπικού χαρακτήρα να τύχουν νόμιμης επεξεργασίας, απαιτείται σε κάθε περίπτωση, ασυνδέτως δηλαδή προς συγκεκριμένο πρόσωπο, να συντρέχουν σωρευτικά οι προϋποθέσεις του άρθρου 4 παρ. 1 του Ν. 2472/1997, που, μεταξύ άλλων, ορίζει ότι τα δεδομένα πρέπει να

[8] Βασίλης Σωτηρόπουλος, «Η συνταγματική προστασία των προσωπικών δεδομένων», σελίδα 105, 2006, Εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη
[9] Ν. 2472/1997 άρθρο 2 εδ.ζ

συλλέγονται κατά τρόπο θεμιτό και νόμιμο για σαφείς και νόμιμους σκοπούς.

Συνεπώς, όταν εκτελείται από δημόσια αρχή επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει αυτή να προβλέπεται ειδικώς από διάταξη νόμου, σύμφωνη με το Σύνταγμα, άλλως η επεξεργασία είναι μη νόμιμη και επιβάλλεται η διακοπή της, ανεξάρτητα από τυχόν παρέμβαση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[10].

Παρόλο που ο νόμος 2472/1997 καθιστά ευχερέστερη την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην περίπτωση εκτέλεσης έργου δημοσίου συμφέροντος που εκτελείται από δημόσια αρχή αφού δεν απαιτεί την συγκατάθεση του υποκειμένου ως προς αυτή, αλλά την προηγούμενη ενημέρωση του, το υποκείμενο των δεδομένων εξακολουθεί να διατηρεί απέναντι στην διοίκηση τα λοιπά δικαιώματα που ο νόμος του κατοχυρώνει δηλαδή

1. το δικαίωμα ενημέρωσης του υποκειμένου αναφορικά με τις λεπτομέρειες της επεξεργασίας κατά το στάδιο συλλογής των δεδομένων προσωπικού χαρακτήρα[11]

2. το δικαίωμα πρόσβασης του υποκειμένου στα δεδομένα καθεαυτά αλλά και στις διεργασίες που έχουν πραγματοποιηθεί επι αυτών[12]

3. το δικαίωμα αντίρρησης[13] του υποκειμένου στην επεξεργασία των δεδομένων που το αφορούν και τέλος

[10] Απόφαση του ΣτΕ υπ' αριθμόν 2281/2002
[11] άρθρο 11 ν. 2472/1997
[12] άρθρο 12 ν. 2472/1997
[13] άρθρο 13 ν. 2472/1997

4. το δικαίωμα της προσωρινής δικαστικής προστασίας σε σχέση με την εφαρμογή μιας πράξης ή απόφασης που τον θίγει[14]

Το πρόβλημα που δημιουργείται έχει ως εξής : με την χρήση της ψηφιακής τεχνολογίας, η αυτόματη δημιουργία ψηφιακών αντιγράφων των αρχείων που χρησιμοποιούνται είναι σε μεγάλο βαθμό αναπόφευκτη. Αυτό πρακτικά σημαίνει ότι τα δεδομένα του ατόμου που τίθενται σε επεξεργασία, μεγάλο μέρος των οποίων είναι προσωπικά, παύουν να βρίσκονται υπό τον έλεγχο του υποκειμένου που αφορούν γεγονός που με την σειρά του έχει πολύ σημαντικές συνέπειες

Α)το υποκείμενο των δεδομένων χάνει σε μεγάλο βαθμό την δυνατότητα ελέγχου των ατόμων που έχουν πρόσβαση σε αυτά και αυτό με την σειρά συνεπάγεται την προσβολή της συνταγματικά προστατευόμενης πληροφοριακής ιδιωτικότητας του πολίτη[15]. Η προσβολή της ιδιωτικότητας πραγματοποιείται είτε από μη νομιμοποιημένη πρόσβαση από υπαλλήλους δημοσίων υπηρεσιών είτε από κακόβουλες επιθέσεις τρίτων προσώπων σε συστήματα που λόγω της εκτεταμένης διασύνδεσης παρουσιάζουν πλείστα τρωτά σημεία σε επιθέσεις τρίτων.

Β)Συνεπακόλουθα, περιορίζεται η δυνατότητα του υποκειμένου να επιτρέπει ή να αποτρέπει την επεξεργασία των προσωπικών του δεδομένων

Γ)Το δικαίωμα του υποκειμένου να ενημερώνεται για την επεξεργασία των δεδομένων που το αφορούν καθώς και να εναντιώνεται σε αυτήν αποδυναμώνεται αισθητά. Με άλλα λόγια,

[14] άρθρο 14 ν. 2472/1997
[15] Βασίλης Σωτηρόπουλος, «Η συνταγματική προστασία των προσωπικών δεδομένων», σελίδα 105

η χρήση των προσωπικών δεδομένων του ατόμων η οποία πραγματοποιείται λόγω έλλειψης τοπικής και χρονικής συνάφειας, σε απόσταση από το υποκείμενο τους συνεπάγεται την αποδυνάμωση των δικαιωμάτων που ο φορέας έχει σε σχέση με αυτά.

Συμπερασματικά λοιπόν, θα μπορούσαμε να καταλήξουμε στα εξής : η χρήση των ψηφιακών ταυτοτήτων θα πρέπει να μεθοδευτεί κατά τρόπο τέτοιο ώστε να δοθεί σύννομη απάντηση στα δύο βασικά προβλήματα που τίθενται από την αξιοποίηση του βασικού χαρακτηριστικού της που είναι η έλλειψη της τοπικής συνάφειας δηλαδή α)να υιοθετηθούν κατάλληλοι μηχανισμοί πιστοποίησης αμφότερων των μερών δηλαδή της διοίκησης και του πολίτη και β)η διαχείριση των προσωπικών δεδομένων που θα πραγματοποιηθεί μέσω των ψηφιακών ταυτοτήτων να βαίνει παράλληλα προς το πνεύμα του νόμου που αφορά την προστασία των προσωπικών δεδομένων.