Considérations sur la Nécessité d'introduction des Dates Biométriques dans les Documents de Voyage

Bogdan Ciucă[1], George Schin[2], Sandu Tirim[3]

[1]*Université Danubius Galati, Faculté de Droit*

[2]*IPJ Galati*

[3]*IPJ Galati*

Abstract: Identity theft has become a growth industry and organized crime threatens to trigger trade disputes between countries of the world. Forgery of administrative documents, in particular payment instruments, documents of identity and travel documents are used for national and transnational criminal activities. In the category of identity papers and travel bulletins are included identity, identity cards and passports. The common goal of the biometric identification is followed to prevent the entry into the territory of the States of the terrorists, drug traffickers, counterfeit cards, identity documents and travel.

Keywords: biometric identification, identity documents, identity papers and travel bulletins

I. L'apparition du faux

L'apparition du faux dans le monde est probablement aussi ancienne que l'émergence de l'écriture. L'usurpation d'identité est devenue un véritable secteur de croissance et de la criminalité organisée menacent de déclencher des conflits commerciaux entre les différents pays du monde. La falsification de documents administratifs en particulier les instruments de paiement, les documents d'identité et de documents de voyage sert aux activités criminelles nationales et transnationales.

Dans la catégorie des documents d'identité et de voyage sont inclus les bulletins d'identité, les cartes d'identité et les passeports.

Les citoyens roumains résidant en Roumanie qui sont mis en droit par le bulletin d'identité, l'attestation d'identité ou de carte d'identité provisoire qui doivent être authentiques: la validité, la corrélation entre l'apparence et la personne la photo apposée sur l'identité qui légitiment l'existence des éléments de protection ou de sécurité, y compris la manière d'attacher une photo et l'application du cachet ou timbre[1].

Sur le plan international on a mis en question le fait que la carte d'identité et le passeport ne devraient être envisagée que la valeur des pièces justificatives de l'identité de toutes les démarches administratives.

[1] V. Berchesan, La Varorisation scientifique des traces de l'infraction, Ed « Little Star », Bucarest, 2003, p. 152

Ainsi, on discute de plus en plus intense concernant les bulletins d'identité et les passeports qui devraient contenir des données biométriques.

Les premiers systèmes biométriques ont été introduits commercialement dans les années 1970. Ceux-ci constituaient un simple scan de la main afin de mesurer la longueur des doigts.

Le terme de la biométrie a été introduit dans le vocabulaire scientifique à la fin du siècle XIX siècle. (biometry ou de la biometrics pour les auteurs américains est un système de statistique)[2].

En France, la plupart des auteurs de spécialise définissent la biométrie comme étant une science qui utilisant des formules mathématiques fait une statistique en ce qui concerne les variations biologiques a l'intérieur d'un groupe déterminé.

On connaît le fait que la biométrie est une méthode traditionnelle d'identification des individus utilisant des moyens scientifiques et techniques modernes ayant comme base les caractéristiques anatomiques et comportementales de ceux-ci. Ces caractéristiques doivent être universelles, uniques, permanentes, collectives et mesurables.

Le but final du système biométrique est l'authentification et la vérification, l'identification ou le codage des données qui permettent d'obtenir une clé biométrique.

L'authentification biométrique de l'individu est la recherche d'un "un contre un» pour démontrer qu'un porteur de document est aussi le titulaire légitime. Pour le succès de ce travail Jean-René Leucerf présentait en France, deux solutions:

1. une carte biométrique sans fichier central. Si les empreintes digitales d'une personne figurent sur la carte certainement que cette personne est le véritable propriétaire de celle-ci. L'utilisation de données biométriques ne permet pas d'assurer l'unicité de l'identité, le même individu pouvant avoir de multiples identités.
2. une carte biométrique avec un fichier unidirectionnel, la situation ou partant de l'identité d'une personne est possible se retrouver les données biométriques, la situation inverse n'étant pas possible. Dans ce sens il a énoncé trois avantages- si le document est imité ou changé, l'identité du porteur peut être vérifiée en sélectionnant son identité dans la base des données, puis faisant la comparaison de ses empreintes avec celles de la base de données biométriques correspondantes a l'identité affichée;
    - Délivrance ou modification d'un document est de simplifiée et sécurisée, sélectionnant l'identité afin d'obtenir une caractéristique biométrique qu'il compare avec celle du porteur;
    - l'unicité de la délivrance du document est assurée au moment de l'émission. Si l'individu a déjà un autre instrument délivré sous une autre identité, les données biométriques sont déjà enregistrées dans la base de données et le système le détecte.

La biométrie pour identification consiste dans la comparaison des données biométriques anonymes avec celles obtenues dans la base des données avec le but de retrouver l'identité de la personne dans une telle dite recherche « un contre un »

L'identification assure l'unicité de l'identité mais ont aussi d'autres utilisations:

- l'identification de la population amnésique, d'une personne désorientée, qui souhaite s'échapper ou disparaître, ou des cadavres dans le cas des catastrophes naturelles majeures

[2] E. Stancu, Traite de criminalistique, édition II revue et ajoutee, Ed. « L'Univers Juridique » Bucarest, 2002, p. 320

- l’identification d’une une personne qui refuse de présenter des documents d'identité, au cas d’un contrôle;
- l’identification d’une personne à partir de vestiges retrouvés à l'endroit d’un crime.

Afin d’éviter les erreurs on a propose dans ces domaines quelques solutions :

- Ne pas abandonner les systèmes de sécurité traditionnels qui permettent d'authentifier le document en l'absence d'équipements biométriques;
- Pour utiliser au moins deux données biométriques afin de tenir compte de certains groupes particuliers tels que les personnes avec les doigts qui ont été coupés ou qui ont le relief papillaire détruit;
- maintenir un travailleur dans la phase essentielle de l'enregistrement des données et le système pour faciliter l'acceptation de la biométrie[3].

Les techniques biométriques sont classés en trois catégories, à savoir:

1. techniques biométriques basées sur l'analyse de traces biologiques (odeur, salive, urine, ADN, sang, etc);
2. Techniques biométriques basées sur l'analyse du comportement (signature, la presse du clavier);
3. Techniques biométriques basées sur l'analyse morphologique (empreintes papillaires, la forme, le visage caractéristiques, l'iris, la rétine)
4. D'autres auteurs classent les systèmes biométriques en deux catégories:

1. systèmes statiques (empreintes papillaires, la géométrie de la main, le visage caractéristiques, l'iris);
2. systèmes dynamiques (voix et la signature)[4].

La technique biométrique est basée sur ce que nous sommes (c'est-à-dire un visage unique, empreintes uniques, etc.) au cours de la vie, peut être mesurée par des méthodes différentes révélé nous convaincre que son utilisation est nécessaire à la fois d'établir un record de personnes à l'identification et de limiter l'accès aux personnes dans les différents domaines de risque ou avec des dispositions spéciales ou d'accéder à différents services.

Les techniques biométriques permettent:

- Identification par la comparaison du visage de la personne présente au point d’identification avec celles enregistrées dans la base de données
- La vérification par comparaison de l’identité déclarée avec les identités associées a la base des traits du visage mémorisé
- Instantané qui permet le suivi d'une personne en séquences vidéo;
- la surveillance qui permet de trouver en temps réel d’une personne dans une séquence vidéo en partant d’une liste d’envisagements

[3] Jean-Rene Lecerf, Mission d’information de la commission des Lois sur la nouvelle génération de documents d’identité et fraude documentaire.
[4] E. Stancu, G. Matei, „Evolutions dans les systèmes d’identification biométriques Nord-Américaines » dans le Rôle et la Contribution des preuves criminalistiques et médico-légales dans l’établissement de la vérité, Ed. Luceafarul, Bucarest, 2005, p. 53

Les données biométriques doivent être contrôlés et identifiés. La vérification consiste à comparer l'actuel point d'échantillonnage de contrôle biométrique des données biométriques enregistrées à partir d'une seule personne.

Le résultat peut être celui d'accepter ou de ne pas accepter le système de comparaison qui doit être positif lorsque la personne est reconnue et négatif lorsque la personne n'est pas reconnue par le système.

Il ya des situations où on doit établir les concordances possibles entre l'échantillon présenté pour un individu et les données enregistrées des autres individus.

Ces techniques ont été développées, mais le principe reste le même: c'est l'étude d'un comportement biologique, ou d'une personne à réduire de manière significative le nombre de coïncidences points, les résultats sont conservés pour référence, un code, puis de déterminer si les coïncidences, la comparaison une fois terminée identité est établie.

La menace croissante du terrorisme requière la mise en œuvre de techniques biométriques plus complexes, qui pourraient aider à l'identification des personnes, la sécurité des institutions de l'État ou les personnes à risque, des frontières ou en criminologie.

Pour accéder à une zone donnée en utilisant des cartes, des passeports pour l'identification des personnes franchissant la frontière, les situations dans lesquelles un travailleur doit vérifier ces documents. La technologie biométrique qui permet l'utilisation d'appareils qui exigent la présence physique de la personne au point de la diminution de l'identification des risques et de fournir une autre personne avec un faux passeport. L'appareil installé à cet effet dans les points d'identification peut travailler sans être surveillé.

Le transit des personnes dans les points de franchir la frontière de plus en plus grand, le danger du terrorisme, et la spécialisation du personnel dans les différents types de faux imposent d'autres mesures de sécurité aux points de passage frontaliers et améliorer la conformité et la sécurité des éléments concernant la délivrance des documents de voyage.

Roumanie va introduire des cartes d'identité biométriques et voyage, mais cela implique des coûts pour l'organisation des points d'identification.

Le système actuel lecteur de passeports peut détecter un grand nombre de faux documents, mais ne peut pas détecter si une personne a utilisé un passeport faux, alors que le système biométrique peut reconnaître si la personne est la même que celle du passeport, mais il ne peut pas vérifier si un document est faux.

Sur le plan international la biométrie est une partie intégrante de nombreux projets de restauration ou de création de documents d'identité, comme la Belgique, la Nouvelle-Zélande, Canada, Australie, Pays-Bas, où l'objectif est de sécuriser les transactions bancaires, mais aussi en France, où la création carte d'identité électronique appelé "INES" connaît une phase de test en Aquitaine.

Projet à l'échelle européenne, en plus d'une base de données ADN à l'utilisation du fichier de police, le problème de l'utilisation des données biométriques sur les passeports et d'identité pour les titres de chacun des membres de l'Union n'est pas à jour. L'augmentation de la pression sur le partenaire américain dans l'U. S. Visa Waiver Program (programme de délivrance de visas) met en question l'obligation de la question du fait que les citoyens devraient avoir: les passeports biométriques de reconnaissance faciale qui comprennent des données.

A partir de la date de 11 Septembre 2001 " le département de la sécurité du pays" américain a une politique fondée sur le développement et la mise en œuvre de la biométrie dans tous les secteurs économiques, ayant une évolution spectaculaire en termes de sécurisation de la frontière.

Depuis Janvier 2004 les passagers qui ont besoin d'un visa pour entrer aux États-Unis doivent se soumettre à un contrôle pour la capture des données biométriques: les caractéristiques du visage et les

empreintes digitales. Depuis septembre de la même année cette mesure a été étendue au-delà des 27 pays comme l'Italie, Luxembourg, Angleterre, Japon, Australie, etc.

Des dispositifs biométriques (dans une amélioration continue) sont opérationnels dans les principaux points d'entrée dans ces pays en vue de la généralisation à toutes les frontières, les aéroports, les ports, les points de passage terrestres, etc.

L'objectif commun suivi est d'empêcher l'entrée sur le territoire de ces Etats les terroristes, les trafiquants de drogues, de contrefaçons de cartes, documents d'identité et de voyage.

Depuis Décembre 2002, Air France met à l'essai une technique qui utilise les empreintes digitales biométriques à l'aéroport Roissy Charles de Gaulle. Cette expérience est basée sur volontariat, objectif étant celui de s'assurer qu'ils ont correctement enregistré les bagages qui se sont engagés dans l'avion. L'empreinte digitale est révélée par un petit dispositif électronique installé sur le compteur d'enregistrement, la comparaison est faite au moment de l'accès à bord.

Toujours en 2004, les systèmes de reconnaissance de l'iris ont été placés dans 10 aéroports du Royaume-Uni, les voyageurs étrangers doivent avoir une photographie de l'iris pour alimenter une base de données.

Nommé Bioort FS-100 est un appareil qui se compose d'un scanner pour identifier les empreintes digitales, un ordinateur et le programme de fonctionnement. En Angleterre, le fichier national comprenant les empreintes papillaires est Nafis, celui-ci permet la lecture directe et aussi des fiches de travail. En Allemagne, le fichier national s'appelle INPOL coordonné par la police fédérale et tous les commissariats de police de Japon sont doués avec des bornes de vérification des empreintes digitales.

En termes de coopération internationale fonctionne le système EURODAC premier dépôt d'empreintes digitales, commun dans trois pays européens: Suisse, Norvège, Islande.

Ce système fonctionne afin d'enregistrer les demandeurs d'asile et immigrants en provenance d'autres États sur la base d'empreintes digitales. Il se compose d'une unité centrale de traitement pour comparer les empreintes digitales géré par la Commission européenne, une base de données centrale d'ordinateur comprenant environ 2 millions d'émigrants candidats et moyens de sécurité de transmission entre les États et la base de données.

La communication de données se réfère à l'état d'origine, lieu et date de contrôle, le sexe et le numéro de référence. Les informations personnelles comme le nom et prénom ne sont pas en référence.

Les empreintes modèles ne sont pas conservées de manière visible mais par une représentation mathématique, ce qui rend que le risque de contrefaçon, le piratage soit être minime. En 2003, dans le EURODAC[5] ont été installés et des zones pour l'enregistrement, la numérisation des empreintes digitales (des doigts et des mains), avec la délimitation de la zone de mémoire directement sur la paume des mains ou sur des feuilles de travail.

En Mai 2003 un groupe d'experts de haut niveau a été créé co-présidé par la France et les États-Unis ayant comme objectif le placement rapide des techniques biométriques, l'objectif commun étant la lutte contre le terrorisme.

En Juin 2003, le groupe des États membres du G8 (les pays les plus industrialisés: États-Unis, l'Allemagne, le Japon, la Grande-Bretagne, France, Italie, Canada et Russie) a décidé d'intégrer la biométrie dans les passeports et les visas pour les ressortissants. La technologie conserve les empreintes digitales ou la reconnaissance selon l'iris.

L'état actuel de la technologie et les résultats spectaculaires obtenus dans le traitement de l'analyse mathématique des images, ont permis le développement et l'application dans la gestion courante de

[5] Représente le système central européen de stockage des empreintes des sollicitant en vue de l'application du Règlement Dublin I, règlement qui établit le pays responsable avec la vérification d'une demande d'asile.

l'autorité judiciaire de l'identification automatique des empreintes digitales (Automated Fingerprint Identification System), systèmes trouves a présent dans une expansion continue.

Une fois avec l'introduction des ordinateurs électroniques dans divers domaines cette technique nouvelle a commence à être appliquée aussi en ce qui concerne l'examen des traces et des impressions papillaires.

En ce qui concerne l'identification des auteurs par l'examen des traces papillaires découvertes sur la place, les systèmes permettent le cryptage et le stockage au niveau central des cas sur le territoire entier, y-compris des traces imprimées de manière fragmentaire.

Se trouvant face à face avec la quantité de données recueillies et la complexité des questions et des cas traités, l'être humain ne peut pas se baser uniquement sur sa mémoire et ses facultés de raisonnement. L'ordinateur s'intègre dans sa démarche, l'assiste dans les questions qui requièrent une capacité de mémoire, une puissance de calcul et des connaissances de spécialité qu'il ne peut pas détenir.

L'utilisation de ce système permet une meilleure coopération internationale, permettant l'identification des auteurs qui ont commis des crimes sur le territoire d'autres États, et des poursuites qui utilisent des documents ou déclarent de fausses identités.

Le service de police d'Ottawa utilise un programme d'enregistrement des empreintes digitales pour les enfants, auquel peuvent participer toutes les personnes intéressées en spécial les parents. Ils peuvent communiquer avec la police afin de se procurer une brochure avec des conseils à cette fin et sont en mesure d'amener les enfants à prendre les empreintes digitales qui seront stockées dans un fichier à la police avec une photo récente ensemble avec les données concernant l'identité de la personne avec numéro de téléphone, le médecin de famille, du dentiste et aussi les noms des amis de celui-ci.[6]

De tels programmes se déroulent partout à travers le monde visant à améliorer la sécurité de la personne qui est de cette manière conseillée de participer de manière active a l'éducation des enfants tel qu'ils ne s'exposent pas aux enlèvements qui sont assez fréquents dans le monde entier.

II. Techniques biométriques

a) Nous savons déjà que les empreintes digitales permettent l'établissement de plus de 150 points caractéristiques. Cette technique représente plus d'un tiers du marché mondial et est spécialement la favorite des autorités françaises.

Comme chaque technique, celle-ci a aussi ses propres limites. Un tel cas s'est produit dans le Massachusetts où une personne a passe 3 ans de prison pour un crime qu'il n'a pas commis (la condamnation a été basée sur l'empreinte papillaire). Après la réalisation de test d'ADN a été prouve le fait que l'individu condamne n'était pas l'auteur du crime.

A l''idée d'un chercheur japonais les hackers Allemands mettent en place une technique de fabrication (fausses empreintes digitales à l'aide du latex). Ces empreintes ont été scannées et comparées avec les empreintes digitales prélevées des gens vivant de la base de données

Mais cette lacune peut être éliminée par l'utilisation de techniques plus efficaces. En ce sens, je donne un exemple proposé par le système suisse.

Celui-ci contient un appareil photo qui peut être connecté à un ordinateur. L'individu met ses doigts sur une plaque de verre, les doigts enregistrés (jusqu'à 150). La chambre de réception bénéficie des rayons

[6] Service de Police d'Ottawa, *„Empreintes digitales pour les enfantes*" http:ottawa police.ca/fr/crime-prevention/child-print/index.cfm

infrarouges et permet le contrôle de la fréquence cardiaque, ainsi on peut vérifier si les doigts appartiennent a une personne vivante ou décédée.

Dans la pratique, cette technologie pour capturer une image de l'empreinte peut être atteint en mettant doigt personne présente au point de contrôle sur l'analyse de récupérer l'image. L'image de l'empreinte est codée en utilisant un algorithme mathématique et est alors insérée dans la base de données. Ainsi, on peut faire une identification soit une vérification.

b) la reconnaissance des individus en fonction de la taille des mains est basée sur les caractéristiques générales des mains (90%), tels que la longueur des doigts. Cette technique a été considérée comme moins fiable, car mesurées ces parties du corps sont plus sensible aux variations causées par des années qui passent. Néanmoins, représente 26% du marché mondial.

c) la photographie de l'iris représente 11% du marché et suit tous les points de coïncidences, mais avec des investissements plus grands que millions d'euros.

L'iris commence à se former dans le troisième mois de grossesse, et des traits distinctifs sont formés jusqu'au huitième mois. Celui-ci a de nombreuses fonctionnalités, bien qu'il soit très petit, 11 mm, dont la variabilité entre les individus est très élevée.

La capture d'image de l'iris peut se faire de deux façons: une manière active lorsque l'utilisateur a besoin de se tourner vers la chambre de l'appareil photo à une distance d'environ 15-35 cm et une manière passive qui suppose l'existence de plusieurs chambres a photographier qui se focalisent contre l'iris.

d) le scan de la rétine est basé sur le dessin des vaisseaux sanguins ayant à la base plus de 400 points de coïncidence.

Le premier problème majeur de cette technique se produit dans des situations où la personne présente à l'identification du port des lentilles de contact, et le second, il s'agit de fermer les yeux à quelques centimètres de la capture.

La capture et le traitement des caractéristiques de la rétine se déroulent en trois étapes. La première personne est placée à une distance inférieure d'une caméra vidéo. Une lumière infrarouge à partir d'une faible intensité est projeté sur la rétine, les vaisseaux sanguins absorbent la lumière à une vitesse supérieure que les tissus environnant l'œil, et la lumière infrarouge avec l'image de la rétine est renvoyée à une caméra vidéo. Le modèle de la rétine capturé est transforme dans un code[7].

e) la reconnaissance du visage examine plusieurs aspects de la face toujours considérés comme invariables (hauteur des joues, les coins de la bouche). Représente 15% du marché mondial.

f) Cela présente caractéristiques qui peuvent être travaillées partant de toutes les sources de types d'image (photo, vidéo) tantôt qu'au monde on abuse de cameras, les unes discrètes, les autres situées a vue.

C'est un système confortable pour le public puisqu'il ne sollicite pas la coopération de l'utilisateur, pouvant travailler à distance. L'utilisation des cameras présente aussi des inconvénients. On peut dépasser légèrement, toute modification du visage ou un accessoire ajoute a celui-ci, peut affecter le résultat du procès d'identification.

Cette technique implique: la détermination c'est-a-dire l'emplacement de la personne face à une image captée par une caméra, l'isolation d'autres objets, les caractéristiques de la forme du visage et puis leur reconnaissance c'est-a-dire la comparaison de l'image captée avec une autre image trouvée dans la base des données[8].

[7] E. Stancu, G. Matei, œuvres lus., p.54-55.
[8] E. Stancu, G. Matei, œuvres lus., p.54-55.

g) techniques de contrôle de la dynamique telle que la presse des tastes (la dureté de la presse, la fréquence des erreurs, la dure de la presse, la durée et la pression avec laquelle on presse certaines tastes) et les traces laissées par la signature représente 30% du marché et la reconnaissance vocale représente 10% du marché (permet l'établissement des différences entre les sexes mais cette technique a comme inconvénient qu'une raucité de la voix ou une intervention chirurgicale peut altérer la voix).

h) Certaines techniques sont basées sur caractères de type visuel, tels que : la géométrie de l'oreille, le dessein des lèvres, la forme des pores sur la peau étant attachées et l'analyse des traces biologiques (sang, salive, ADN). Ces techniques sont en cours d'élaboration.

i) La technologie d'identification de la voix suppose que la personne se trouve devant le dispositif afin de créer un modèle de la voix[10] qui conduit a l'identification. Cette personne doit dire quelques phrases à plusieurs reprises afin de construire le modèle.[9]

[9] Nomme aussi template.