Droit d'@ccès

LE COURRIER DE LA COMMISSION DE CONTRÔLE DES INFORMATIONS NOMINATIVES

N°3
Juillet 2006

Édito

2005, 4 octobre, Monaco devient le 46e Etat membre du Conseil de l'Europe.

2006, 3 mars, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales entre en vigueur en Principauté.

2007, Monaco participera à la première journée européenne pour la protection des données à caractère personnel.

Rendez-vous le 28 janvier 2007.

Sommaire

L'informatisation des données au travers de la réglementation monégasque ..... p. 2

Les étiquettes intelligentes ..... p. 2

Le droit d'accès : quésaco ..... p. 4

Exercer son droit d'accès ..... p. 5

Les lignes d'éthique ..... p. 6

L'utilisation des informations nominatives vue par le Cinéma ..... p. 8

Protection des données personnelles : quelques exemples concrets

On retrouve les données personnelles au centre de sujets développés dans nos quotidiens et autres journaux et magazines :

A Nice, le CHU suit les patients grâce à un bracelet électronique

"Les patients portent un bracelet muni d'un code-barres pour faciliter leur identification".
01 Informatique - 6.01.2006

En France, le casque des gendarmes muni d'une caméra

"Une caméra miniature cachée dans le casque de gendarmes à moto habillés en civil (...) afin de filmer discrètement les infractions des automobilistes (...). L'automobiliste (...) reçoit ensuite un PV à son domicile, comme les radars traditionnels."
Nice-Matin - 05.01.2006

Aux Etats-Unis, la fiabilité du fichier du FBI comprenant les empreintes digitales des criminels et suspects montrée du doigt

"Les empreintes digitales d'un avocat (...) et celles retrouvées sur un sac contenant des détonateurs ayant appartenu aux auteurs des attentats de la gare d'Atocha, à Madrid, en mars 2004, étaient identiques."
Eric Leser - Le Monde - 13.01.2006

Au Canada, des puces électroniques pour la sécurité routière

Le directeur de la sécurité routière de l'Université Laval à Québec estime qu'il "faudrait remplacer nos vieilles plaques d'immatriculation par de nouvelles, dotées d'une puce électronique dont les informations seront lues par lecteurs installés en bordure de routes."
Eric Thibault - Le Journal de Québec relayé par canoë.com - 23.03.2006

L'informatisation des données au travers de la réglementation monégasque

- *En 2006, la protection des données s'est trouvée renforcée par les ordonnances souveraines N°408 à 412 du 15 février 2006 publiées le 3 mars 2006 qui ont rendu exécutoire en Principauté la CONVENTION EUROPEENNE DE SAUVEGARDE DES DROITS DE L'HOMME ET DES LIBERTES FONDAMENTALES du Conseil de l'Europe.*

- *Article 8 (1) "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance".*

- *En 2005, les articles 9 et 10 de l'arrêté ministériel n°2005-156 du 21 mars 2005 sur le droit d'accès des travailleurs exposés à l'inhalation de poussières d'amiante à la liste établie par le chef d'entreprise précisent que ce document mentionne la nature de leur activité, les niveaux d'exposition et la durée de cette exposition. Leur dossier médical est conservé à l'Office de la Médecine du Travail pendant quarante ans après la cessation de l'exposition.*

Des étiquettes intelligentes qui parlent de vous...

Les étiquettes, codes barres et autres marquages de produits ne s'expriment pas ; mais ils peuvent communiquer entre eux.

Le principe des RFID

Cette nouvelle technologie consiste à placer sur un produit un marqueur, appelé TAG ou étiquette électronique, qui ressemble à un ensemble de composants électroniques écrasés.

Ce TAG comprend une puce électronique et une antenne qui permettent de mémoriser des informations et de les transmettre à distance -non plus par lecture optique comme les codes barres- mais par radiofréquence.

Le RFID se met au service de la lutte contre la contrefaçon dans le football. Pendant la Coupe du Monde de Football 2006, les billets ont été munis d'une puce RFID. Les visiteurs ont passé leur billet à proximité d'un lecteur intégré aux tourniquets qui donnaient accès aux stades. Le lien entre le billet et la personne qui l'avait acheté s'est fait au niveau de la plate-forme de contrôle de la FIFA.

D'ici à quelques mois, les maillots de la Juventus vendus aux amateurs de foot seront munis de ces puces cousues sur le col du maillot avec une mention d'information.

L'intérêt des étiquettes intelligentes et où les trouve-t-on aujourd'hui ?

Pour sécuriser les frontières et la circulation des voyageurs, les Etats ont progressivement intégré des données biométriques dans les passeports. A l'intérieur de la couverture se loge une puce RFID.
En 2005, afin d'optimiser le fonctionnement de sa chaîne logistique, la Poste britannique a mis en œuvre des RFID pour suivre les flux de courriers et repérer, pour mieux les corriger, les problèmes d'acheminement.

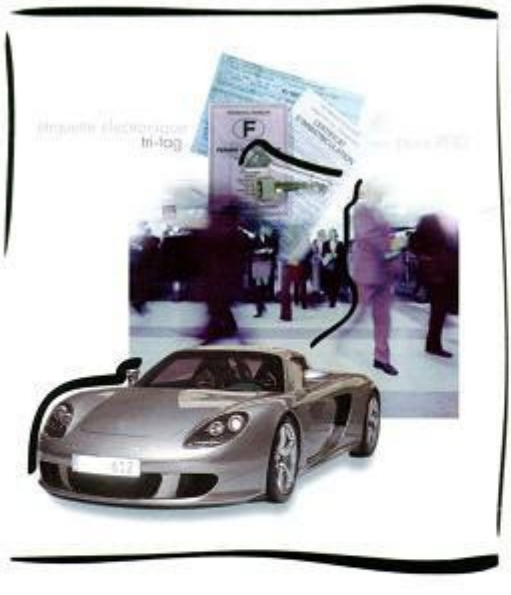
Mais aussi la puce sous-cutanée...

En février 2006, deux salariés d'une entreprise de sécurité américaine se sont fait implanter une puce RFID, grosse comme un grain de riz, sous la peau. Cette société souhaitait sécuriser les accès des pièces où sont stockées les images destinées, en cas de besoin, aux services de police. Le responsable de cette entreprise a opté pour le RFID considérant les systèmes d'accès par biométrie trop onéreux.

Les étiquettes intelligentes se vulgarisent, demain, elles vous "parleront" !

Les codes barres sur les produits ont encore quelques belles années devant eux car les TAGS sont encore d'un coût non négligeable, entre 30 à 40 centimes d'euros par marqueur (puce et système d'exploitation).
Toutefois, les projets des industriels vont bon train :

- Le "tri-tag" **appliqué au véhicule** a pour principe de disposer 3 tags sur une voiture : un sur le pare-brise, un sur les plaques d'immatriculation, un sur la carte grise du propriétaire. Ainsi, s'allient lutte contre le vol de voitures et lutte contre les excès de vitesse par une identification plus rapide du véhicule.
- Les canadiens se penchent sur un puce RFID sous-cutanée qui pourrait remplacer **les clés de votre appartement**.
- Les japonais ont développé **un chariot** qui, associant les technologies du RFID et des écrans LCD, vous permet tout en faisant vos courses de disposer d'informations sur les produits que vous mettez dans le chariot et sur ceux qui seraient susceptibles de vous intéresser.



Les risques pour la vie privée et les étiquettes intelligentes

Ces étiquettes intelligentes, appliquées aux personnes, à leurs déplacements, à leur comportement de salarié, de consommateur ou autre, soulèvent de redoutables questions au sujet de la protection de leurs données personnelles.

Elles permettent **une identification numérique des individus** et offrent **la faculté d'une traçabilité généralisée et d'un contrôle permanent de la circulation des personnes** au travers des objets qu'elles portent, qui les transportent, qu'elles utilisent, ou encore des supports d'accès dont elles ont l'obligation de se munir.

Derrière cette identification numérique, **les risques de dérives** eu égard à **leur potentiel d'intrusion dans la vie privée** sont inquiétants.
L'évaluation des impacts de ces nouvelles technologies sur la vie privée des personnes est encore embryonnaire.

Leurs développements devront intégrer une dimension "éthique" afin que les personnes qui "porteront" ces étiquettes intelligentes en soient informées et qu'elles puissent décider en toute connaissance de cause de les laisser ou non "actives".

Le droit d'accès, quesaco ?

Quel est l'intérêt du droit d'accès ?

■ Le droit d'accès permet de **savoir** si des informations vous concernant sont exploitées dans un fichier, appelé par la loi "traitement d'informations nominatives", que le fichier soit informatisé ou non.

Ainsi, vous avez la possibilité de connaître, notamment :

- toutes les données vous concernant qui figurent dans un fichier ;
- la raison de leur présence dans ce fichier ou l'objectif recherché par l'exploitation de ces données ;
- à quoi servent ces informations ;
- l'origine des informations qui s'y trouvent, c'est-à-dire qui les a données à l'organisme que vous interrogez ;
- les destinataires (ex. organisme de sécurité sociale) des informations nominatives (ex. nom, prénom, adresse, type de contrat de travail) contenues dans le fichier ; mais aussi des données issues de l'exploitation de ce fichier (ex : temps de travail avec mise en évidence des arrêts de travail et de leur cause) ;
- les transmissions éventuelles vers d'autre(s) organisme(s), dans quel(s) pays et pour quelle(s) raison(s).

■ Le droit d'accès permet de **contrôler** si les informations qui vous concernent sont exactes.

■ Le droit d'accès permet, si de besoin, de **corriger ou de mettre à jour** les informations qui sont inexactes, incomplètes, équivoques ou périmées.

■ Le droit d'accès permet de demander à ce que des informations soient **supprimées**, pour les raisons précédemment énoncées, ou, parce que leur collecte, leur enregistrement ou leur communication est prohibé.

Qui peut exercer le droit d'accès ?

Ce droit est ouvert à :

■ toute personne qui souhaite savoir si un fichier informatique comporte des informations la concernant directement.

■ tout parent, enfant ou petit-enfant, conjoint d'une personne décédée qui souhaite savoir si un fichier informatique comporte des informations concernant le défunt.

■ toute personne morale (ex. une entreprise) qui souhaite savoir si un fichier informatique comporte des informations concernant ses membres.

Le droit d'accès : un droit direct et personnel

Si vous souhaitez exercer ce droit auprès d'un organisme pour savoir de quelles informations il dispose sur vous et ce qu'il en fait, vous ne pouvez pas mandater ou demander à quelqu'un d'autre de le faire.
Vous seul pouvez demander à avoir accès à vos informations.

C'est la raison pour laquelle si vous souhaitez exercer votre droit d'accès, il vous est demandé de justifier de votre identité.

Une exception : l'accès aux données à caractère médical.
Dans ce cas, les informations ne pourront être communiquées qu'au médecin que vous aurez désigné à cet effet (art. 15 chiffre 2 de la loi n°1.165)

Les limites du droit d'accès

Le droit d'accès ne s'applique pas :

■ aux fichiers intéressant la sécurité publique,

■ à ceux dont l'usage relève de l'exercice du droit à la vie privée et familiale.

Le droit d'accès : les bases légales

Le droit d'accès aux informations nominatives est un principe général inscrit dans la loi n°1.165 du 23 décembre 1993 réglementant les traitements d'informations nominatives :

- sur le principe : art. 13 al. 2
- sur les limites : art. 10, 13 & 25
- sur les modalités pratiques : art. 15
- sur la saisine de la CCIN : art. 3 & 18
- sur les sanctions : art. 21 et s.

Des dispositions particulières peuvent être prévues par ailleurs, comme, par exemple :

- dans le cadre de la recherche biomédicale (loi n°1.265 du 23 décembre 2002)
- ou au titre du suivi des travailleurs exposés aux poussières d'amiante (arrêté ministériel du 21 mars 2005)

Exercer son droit d'accès

Comment exercer son droit d'accès ?

Le droit d'accès s'exerce directement auprès de l'organisme public ou privé qui exploite les données.

Une demande claire doit être adressée à cet organisme aux fins d'obtenir communication des enregistrements effectués par ses services.

Selon les organismes, cette demande peut être écrite ou effectuée oralement.

Comment savoir auprès de qui s'adresser dans l'organisme ?

Adressez-vous directement auprès de l'organisme qui détient vos données.

Si votre demande est restée infructueuse, ou si vous souhaitez savoir quel type de fichier informatique existe au sein d'un organisme déterminé, vous pouvez :

- vous adresser au **Secrétariat de la Commission de Contrôle des Informations Nominatives** (CCIN),
- et venir y consulter **le répertoire des traitements.**

Le répertoire des traitements : "le fichier des fichiers"

Ce répertoire est un fichier informatique qui comprend les renseignements fournis par les personnes physiques ou les organismes publics et privés qui exploitent en Principauté des fichiers informatiques contenant des informations nominatives, à l'exception des traitements intéressant la sécurité publique.

En effet, avant d'être exploité, tout fichier informatique de ce type doit faire l'objet :

- pour les personnes de droit privé (ex. entreprise, association), d'une déclaration auprès de la CCIN qui délivre un récépissé de mise en œuvre ;
- pour les personnes morales de droit public (soit l'Etat, la Commune, les établissements publics), d'un avis motivé de la CCIN suivi d'une décision de mise en œuvre.

Ce répertoire comprend pour chaque fichier informatique légalement mis en œuvre, entre autres :

- la date du récépissé ou de la décision de mise en œuvre ;
- l'identité du responsable du fichier ;
- les caractéristiques et la finalité du traitement ;
- le service ou la personne auprès de laquelle peut s'exercer le droit d'accès ;
- les mesures prises pour permettre l'exercice de ce droit ;
- le détail des informations exploitées dans le fichier, avec leur origine, leur durée de conservation et leur(s) destinataire(s).

Ne pas respecter le droit d'accès d'une personne est passible de sanctions pénales.

Que doivent faire les responsables de fichiers ?

Le responsable du fichier doit, **dans le mois qui suit votre demande**, vous répondre. S'il exploite des informations vous concernant, il doit **vous les communiquer gratuitement**, sous une forme "écrite, non codée et conforme au contenu des enregistrements".

S'il refuse ou ne répond pas dans ce délai : vous pouvez saisir le Président de la CCIN par LAR.

S'ABSTENIR VOLONTAIREMENT DE COMMUNIQUER à une personne les informations qui la concernent est passible :
d'un emprisonnement de 1 mois à 6 mois et/ou
d'une amende allant de 9.000 à 18.000 euros (art. 21-2°).

COMMUNIQUER SCIEMMENT des renseignements ou documents inexacts aux personnes intéressées est passible :
d'un emprisonnement de 3 mois à 1 an et/ou
d'une amende allant de 18.000 à 90.000 euros (art. 22-4).

Un fichier informatique particulier : les lignes d'éthique

Les lignes d'éthique ou "WHISTLEBLOWING"

La CCIN invite à la prudence.
La presse a beaucoup parlé au second semestre 2005 des dispositifs d'alerte professionnelle, appelés "lignes d'éthique" ou "Whistleblowing".

L'origine des lignes d'éthique : une loi américaine dite Sarbanes-Oxley

Cette loi du 30 juillet 2002 a pour objet de rétablir la confiance dans le marché financier.

Elle demande aux entreprises cotées en bourse aux Etats-Unis et à leurs filiales étrangères de certifier leurs comptes. Transparence des méthodes de gestion et lutte contre les fraudes en matière comptable et financière sont visées.

Cette loi préconise la mise en place de procédures afin de développer un fonctionnement harmonieux des entreprises dans le respect de son environnement socio-économique, appelé "Corporate Governance".

L'idée : une procedure d'alerte

Une des procédures développées est basée sur un dispositif d'alerte professionnelle.

Ce système permet aux salariés de "dénoncer" à leur hiérarchie des pratiques ou des comportements qu'ils considèrent ne pas être en adéquation avec les dispositions légales en vigueur ou les politiques d'éthique et règlements instaurés au sein de l'établissement.

En théorie limité au domaine financier, le système a été étendu, en pratique, à l'ensemble des activités de l'entreprise.

Comment ça marche ?

La maison mère informe les salariés qu'une adresse postale, une adresse électronique ou, plus généralement, une permanence téléphonique est à leur disposition afin de faire connaître, de manière anonyme ou non, les dysfonctionnements constatés.

Prenons l'exemple de la permanence téléphonique ou "hot line" :

- Un numéro de téléphone, gratuit, accessible 24heures/24, 7jours/7 avec des opérateurs parlant les langues des salariés, est mis à disposition.
- Un salarié peut dès lors téléphoner, de manière anonyme s'il le souhaite, pour "dénoncer" un "écart".
- La hot line saisit son identité, si non anonyme, les motifs de son appel, l'identité des personnes citées dans la conversation "coupable du dysfonctionnement" ou "témoin".
- La hot line transmet à la "Maison Mère" de l'entreprise les informations compilées.
- La "Maison Mère" rédige un rapport sur les évènements cités et le transmet à l'entreprise concernée, par exemple un organisme localisé en Principauté de Monaco.
- L'entreprise monégasque enregistre les informations, réalise ou non une enquête interne, sanctionne ou non le salarié concerné, enregistre ou non des mentions dans son dossier personnel, puis transmet les modalités de gestion de l'alerte à la "Maison Mère".

Il s'agit là, selon le cas, d'un ou de plusieurs fichiers informatiques comprenant des informations nominatives qu'il convient de mettre en œuvre dans le respect des dispositions de la loi n°1.165, notamment, en le ou les déclarant auprès de la CCIN.

Le dispositif de la procédure d'alerte : un traitement automatisé à déclarer à la CCIN

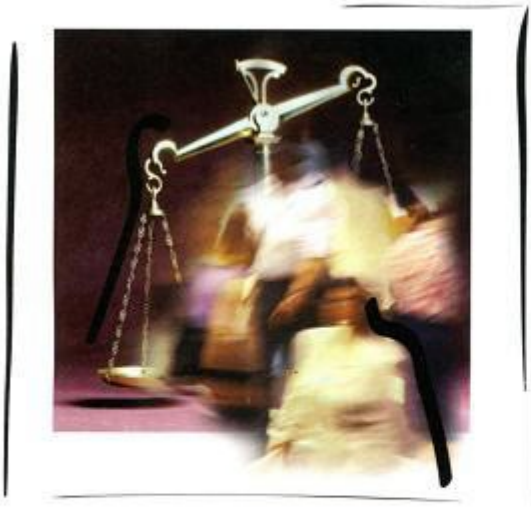
Le dispositif collecte, enregistre des informations nominatives telles que les noms, prénoms, adresses, fonctions des personnes physiques citées.

Par exemple :
- identité et fonction de la personne ayant appelé ;
- identité et fonction des témoins ;
- identité et fonction de la personne accusée ;
- faits "dénoncés" ;
- enquête, conclusions et décision, s'il y a lieu ;

Ainsi, l'instauration de la procédure d'alerte professionnelle induit, bien souvent, la réalisation d'opérations automatisées contenant des informations nominatives, comme :

- la transmission de ces informations,
- l'enregistrement de ces données,
- la collecte d'autres informations à la suite de l'enquête effectuée en interne...

Autant d'informations qui peuvent également être saisies dans le dossier des personnes concernées au sein du service du personnel.



Les lignes d'éthique : danger pour la vie privée

Un préalable à la mise en place de lignes d'éthique : une réflexion globale à mener au sein de l'entreprise afin de ne pas nuire à la vie privée des salariés.

Il convient, notamment, de s'interroger sur :

- **le risque de non respect du principe de présomption d'innocence et des droits à la défense**

Exposés ou non de manière anonyme, les faits dénoncés sont susceptibles de voir déclencher à l'encontre d'une personne des **suspicions**, des **soupçons**, voire une enquête interne pouvant déboucher sur des **sanctions**, sans qu'elle ait pu bénéficier des droits élémentaires de la défense.

- **les risques de dénonciations calomnieuses**

Anonyme ou pas, ces procédures ouvrent la voie à **un système organisé de délation calomnieuse** dans un cadre professionnel avec tous les risques d'instabilité que cela peut induire sur le personnel, dont celui de stigmatisation des salariés.

- **L'absence de garanties offertes par la loi**

Ces dispositifs privés **échappent à tout contrôle et n'apportent pas de garanties** quant à la protection de l'intégrité des personnes alors que d'autres moyens prévus par la loi existent d'ores et déjà pour protéger le respect des dispositions légales et des règles fixées par l'entreprise.

- **L'absence de respect des droits des personnes**

Les dispositifs développent **peu ou pas du tout l'information** et les modalités prévues afin de permettre aux personnes concernées "délateur", "témoin" ou "accusé" d'exercer **leurs droits d'accès, d'opposition, de rectification, voire de suppression.**

Cette absence constitue une violation des principes de loi sur la protection des informations nominatives.

Il est indispensable de prendre ces éléments en compte lors de l'élaboration des procédures d'alerte professionnelle, de les penser avec la plus grande prudence avant de les exposer aux personnes concernées et de déposer la déclaration de mise en œuvre à la CCIN.

L'utilisation des informations nominatives vue par le cinéma

Des scénarii de fiction, des technologies d'agents secrets, le futur vu par le cinéma, c'est aujourd'hui !

1983 *"Jamais plus jamais"*

produit par Warner Bros

"James Bond" doit lutter contre l'organisation criminelle du Spectre qui a pris en "otage" Jack Petachi, officier de l'armée américaine. Opéré, son œil reprend les caractéristiques biométriques du Président des Etats-Unis. Cet iris est une clé d'accès...

"1984"

produit par Virgin & Umbrella films

Il y a 20 ans, Michael Radford mettait en scène ce livre écrit par G. Orwel en 1948. Dans ce monde, chaque domicile, chaque rue est muni d'un "télé-écran", d'un système de vidéosurveillance qui scrute gestes, visages, paroles, comportements... Un homme, Winston Smith, matricule 6079, écrit son journal intime...

1998 *"Bienvenue à Gattaca"*

produit par Jersey film & Columbia Pictures

Dans un monde parfait géré par la génétique et contrôlé par le "tout biométrique", un homme "naturel" prend la place d'un homme "créé" par le système et déjoue la technologie pour arriver à ses fins.

2002 *"Minority Report"*

produit par 20th Century Fox

Steven Spielberg nous emmène en 2054. Ici, les individus sont fichés à grande échelle, l'ouverture des portes du métro se fait par le biais de l'iris, le passage devant un panneau publicitaire d'un voyagiste vous invite, personnellement, à prendre des vacances.

2006

- Du domaine de la pure fiction il y a 20 ans, les techniques de biométrie se développent.

  Si les empreintes digitales ou le contour de la main sont aujourd'hui les plus utilisés, les recherches portant sur l'iris sont nombreuses eu égard, notamment, à l'utilisation de cette "donnée" qui permettrait de déterminer les propensions d'une personne à développer certaines pathologies, utile, notamment, lors des phases de recrutement.

  La biométrie fait déjà partie de notre quotidien : contrôle d'accès aux locaux de travail, aux chambres d'hôtel, aux cantines scolaires, identification des personnes dans les passeports, les cartes d'identité, clés permettant le démarrage des véhicules ou celui d'un ordinateur.

- De même les caméras sont là avec leurs possibilités de visualisation et d'échanges, d'analyses des comportements, appelées "morfing". Elles sont également aujourd'hui installées par les particuliers à leur(s) domicile(s) afin d'assurer la sécurité des lieux, voire de surveiller ce qui s'y passe. Est-ce que "Big Brother" nous regarde ?

- Les opérateurs de téléphonie mobile développent des systèmes qui permettront bientôt à vos portables de vous informer du chemin le plus rapide pour vous rendre à l'enseigne vantée, du prix et des avantages du produit présenté, ou encore, de vous offrir la faculté d'écouter un morceau choisi du spectacle affiché... au gré de vos passages devant des marqueurs placés à bon escient sur des affiches publicitaires.

COMPOSITION DE LA COMMISSION :
Président : Maître René CLERISSI

Membres titulaires : M. Max BROUSSE, Me René CLERISSI, Me Jacques SBARRATO
Membres suppléants : M. Chérif JAHLAN, Mme Pauline MIGLIARDI, M. Renaud RISCH-ROMANI

COMPOSITION DU SECRETARIAT PERMANENT :
Secrétaire Général : Mme Isabelle ROUANET-PASSERON

Chef de Projet : Mme Martine LIBERATORE,
Administrateurs : Mlle Céline ANSQUER, Mlle Caroline PORASSO
Secrétariat : Mlle Emilie CAMPILLO, Mme Anne PRAT

Commission de Contrôle des Informations Nominatives
Bureau 409 - Bloc B - "Gildo Pastor Center" - 7, rue du Gabian - MC 98000 Monaco - Téléphone : (+377) 97 70 22 44 - Fax : (+377) 97 70 22 45
E-mail : ccin@gouv.mc - Site Internet : www.ccin.mc
Les bureaux sont ouverts du lundi au vendredi de 09h00 à 12h30 et de 13h30 à 17h00.
Photos : Gattaca © Columbia Pictures Corporation, Minority Report © UFD, DR.