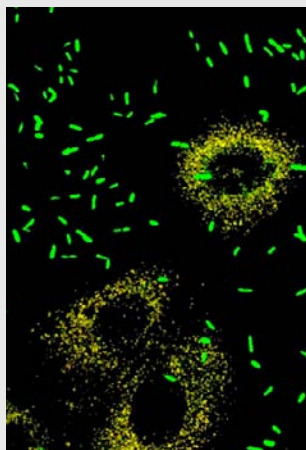


SKIN-O-FLOR

Les bactéries pacifiées



Sur cette image, on distingue nettement, en vert, des bactéries (*Pseudomonas fluorescens*) au contact de cellules de la peau (des kératinocytes, qui constituent 90 % de l'épiderme), en jaune.

Comment combattre le phénomène de «peau sensible», responsable de rougeurs, d'irritations et de tiraillements ? Le projet Skin-O-Flor, cofinancé par l'État et les régions Centre et Haute-Normandie, a pour but de rendre inoffensives les bactéries responsables de ces désagréments en agissant sur les signaux chimiques qu'elles échangent avec la peau.

«La plupart des millions de bactéries présentes sur et à l'intérieur de notre peau sont inoffensives», affirme Marc Feuilloley, directeur du laboratoire de Microbiologie Signaux et Microenvironnement de l'Université de Rouen à Évreux (Eure), qui étudie la communication entre les bactéries et les cellules de la peau. «Mais quelques-unes deviennent

pathogènes lorsqu'elles sont stimulées par les signaux chimiques émis par certaines hormones. Ainsi, lorsqu'une personne est victime de stress ou de dépression, sa peau libère un peptide nommé substance P, qui se diffuse dans la sueur et peut stimuler la virulence des bactéries», explique le chercheur. «Ce phénomène expliquerait certains symptômes cutanés, dont le "syndrome de peau sensible" qui touche environ 50 % des femmes.»

La méthode Skin-O-Flor consiste à bloquer la communication entre les bactéries et la peau pour maintenir son intégrité. «C'est une démarche totalement nouvelle et originale, se réjouit Marc Feuilloley, qui permet de combattre les irritations cutanées sans tomber dans le domaine de

la pharmacie. Car lorsque vous agissez directement sur la peau ou sur les bactéries, vous créez un médicament, un antiseptique ou un antibiotique, qui nécessite une autorisation de mise sur le marché. En revanche, si vous travaillez sur la communication entre les deux, vous êtes efficace tout en restant strictement dans le domaine cosmétique.»

«Nous avons donc testé tout une série de produits cosmétiques, et en avons identifié deux capables de bloquer l'effet de la substance P sur les bactéries.» Ces produits sont l'Eau d'Uriage et le Teflose de BioEurope (groupe Solabia), deux partenaires du projet Skin-O-Flor. D'autres produits de la marque Uriage, dont le Xémose et le Bariéderm, ont bénéficié de ces travaux.



CONTVERRCOL

Flacons : l'ivresse des couleurs

La contrefaçon est un fléau pour l'industrie cosmétique mondiale, en particulier pour la parfumerie. L'une des stratégies pour la combattre consiste à fabriquer des flacons infalsifiables. «Pour cela, nous incluons dans le verre des oxydes métalliques de cuivre, d'or ou d'argent et les précipitons sous formes de nanoparticules», explique Jean-Philippe Blondeau, enseignant-chercheur à l'Université d'Orléans. Son laboratoire, le CEMHTI, est avec le GREMI, l'institut PRISME et l'Université de Cracovie l'un des partenaires du projet ContVerrCol, financé par la région Centre.

Une première application possible de cette technologie est d'utiliser «des particules d'argent visibles uniquement à la lumière ultraviolette. C'est un bon moyen de distinguer les

vrais flacons des contrefaçons». Mais il est plus intéressant encore de colorer le verre localement, en surface ou en volume : les motifs ainsi créés enjolivent les flacons et les rendent pratiquement infalsifiables. C'est l'objet de la technologie mise au point par Jean-Philippe Blondeau et son équipe. «Une méthode consiste à passer un flacon contenant des nanoparticules de cuivre dans un four avec un gradient de température de bas en haut : c'est ainsi que Saint-Gobain fabrique le flacon Fahrenheit de Dior.»

Par ailleurs, la méthode ContVerrCol permet d'aller plus loin. «Notre équipe travaille sur la coloration locale par laser. Elle permet de tracer des motifs en surface et à l'intérieur même du verre, grâce à des échanges entre les ions métalliques – Ag⁺, Cu⁺,

Au⁺ – et des éléments réducteurs tels l'étain ou l'antimoine pour former les nanoparticules.» Il est ainsi possible de dessiner toutes sortes de motifs au cœur du matériau. «Les couleurs obtenues dépendent de l'oxyde utilisé – rouge pour le cuivre, jaune à ambré pour l'argent, rouge à bleu pour l'or – ainsi que de la taille et de la fraction volumique des nanoparticules métalliques.»



Si le four à gradient de température crée des dégradés de couleurs (flacon à droite), seule la coloration locale par laser peut produire des motifs au cœur même du verre, à l'aide par exemple de nanoparticules d'argent (ci-dessus).

POINT DE VUE

Renseignement : le traitement massif de données est aussi dangereux qu'inefficace

Au nom de la lutte contre le terrorisme, la France adopte un dispositif de détection de profils de comportements suspects inopérant, coûteux et menaçant pour la vie privée.

Claude CASTELLUCCIA et Daniel LE MÉTAYER

Au motif de lutter contre le terrorisme, plusieurs pays ont adapté leur cadre juridique pour permettre un traitement massif de données à des fins de renseignement. La France s'est également engagée dans cette voie avec le projet de loi relatif au renseignement, adopté par l'Assemblée nationale en première lecture le 5 mai 2015 et en passe d'être discuté au Sénat à l'heure où nous écrivons. L'objectif affiché de ces dispositions est de doter les États de moyens de détecter des « signaux faibles », autrement dit des profils de comportements suspects qu'il conviendrait de repérer le plus tôt possible pour déjouer des projets terroristes. D'un point de vue strictement technique, on peut cependant s'interroger à la fois sur les risques liés à ces procédés et sur leur efficacité.

Le risque principal posé par un traitement massif de données est celui d'une atteinte tout aussi massive à la vie privée des citoyens. Les promoteurs de ces lois utilisent un double argument pour rassurer les populations : dans un premier temps ne seraient collectées « que » des métadonnées (ou des « données de connexion ») et celles-ci seraient « anonymisées ». Or des données sont considérées comme anonymes s'il n'est pas techniquement

possible de retrouver les identités des personnes concernées.

On ne peut donc pas à la fois prétendre que des données sont anonymes et prévoir en cas de suspicion la levée de cet anonymat. Les données en question sont donc

des personnes et, si leur état civil n'est pas dévoilé dans un premier temps, il pourra l'être ensuite.

Revenons aux données de connexion. L'adresse de la page web à laquelle un internaute souhaite accéder est une donnée de connexion qui fournit souvent autant d'informations que la page elle-même. De manière générale, il est bien connu des spécialistes que les données de connexion sont parfois plus intrusives que les données elles-mêmes. Par exemple, le fait de savoir qu'un appel téléphonique est destiné à un cardiologue ou au bureau des alcooliques anonymes apporte plus d'informations que la conversation en soi, qui peut se réduire à une simple prise de rendez-vous. Autre illustration, l'analyse des données de géolocalisation des taxis new-yorkais a montré qu'elles pouvaient être utilisées pour inférer la religion de certains chauffeurs.

Ce n'est pas vraiment rassurant, mais est-ce efficace ? Pour cette question, un autre mot-clef apparaît de manière récurrente dans les débats, comme un remède magique : l'*algorithme* censé analyser les fameuses données de connexion pour en extraire inexorablement la liste des suspects. Il est vrai que des techniques d'apprentissage ou de classification automatique se révèlent très utiles et efficaces

Le paradoxe des faux positifs
démontre que l'on risque d'identifier des centaines de milliers de « faux terroristes »

au mieux « pseudonymisées », ce qui implique, comme l'a rappelé la CNIL, qu'elles restent couvertes par la loi Informatique et Libertés. L'usage du mot « anonyme » est en l'espèce un contresens : l'objet est bien de collecter des informations liées à