Quand le combustible se fait rare, le cœur de l'étoile s'effondre et libère une énorme quantité d'énergie qui arrache les couches externes de l'étoile dans une explosion de supernova, pouvant laisser derrière elle une étoile à neutrons ou un trou noir. Ces supernovæ créent un vent de particules qui peut gonfler des bulles autour d'un centre galactique.

Nous savons que le centre de la Voie lactée a été une région de formation stellaire intense dans un passé proche. Plusieurs milliers d'étoiles d'à peine six millions d'années entourent la région du trou noir central. Des étoiles suffisamment massives formées à la même période auraient eu le temps d'exploser en supernovæ. Elles auraient alors entraîné un vent de gaz chaud s'élevant de la partie centrale de la Galaxie, un souffle assez puissant pour gonfler les bulles.

Comme nous le voyons, l'histoire des bulles de Fermi est étroitement liée à l'histoire et à l'évolution de la Voie lactée. Les bulles peuvent nous permettre de comprendre les processus physiques par lesquels les trous noirs attirent la matière environnante, et comment les rayons cosmiques de haute énergie interagissent avec le gaz interstellaire. Bien qu'il existe des structures semblables aux bulles de Fermi dans d'autres galaxies, les bulles de la Voie lactée permettent d'étudier ces systèmes de plus près.

L'une des propriétés les plus extraordinaires de ces bulles est qu'elles sont énormes et brillantes en rayons gamma, mais presque invisibles aux autres fréquences. Nous espérons que les nouvelles données du satellite *Planck*, qui a cartographié le rayonnement micro-onde sur l'ensemble du ciel, apporteront des indices importants. Nous essayons aussi de cartographier les bulles en rayons X, mais le champ de vue réduit des instruments actuels représente un sérieux défi pour des structures aussi vastes.

Après la découverte par Galilée de la nature de la Voie lactée, les astronomes ont mis trois siècles pour comprendre que notre Galaxie n'en est qu'une parmi des milliards d'autres. Avec un peu de chance, nous mettrons moins longtemps à comprendre la signification des bulles de Fermi. ■

BIBLIOGRAPHIE

A. Franckowiak et S. Funk, **Giant gamma-ray bubbles in the Milky Way,** *Physics Today*, vol. 67, pp. 60-61, juillet 2014.

W. Atwood *et al.*, ***Fermi* : une fenêtre sur l'Univers extrême,** *Dossier Pour la Science*, n° 71, avril-juin 2011.

Meng Su *et al.*, **Giant gamma-ray bubbles from *Fermi*-LAT : Active galactic nucleus activity or bipolar galactic wind ?**, *The Astrophysical Journal*, vol. 72(2), pp. 1044-1082, 2010.

TRÉSORS de la Terre

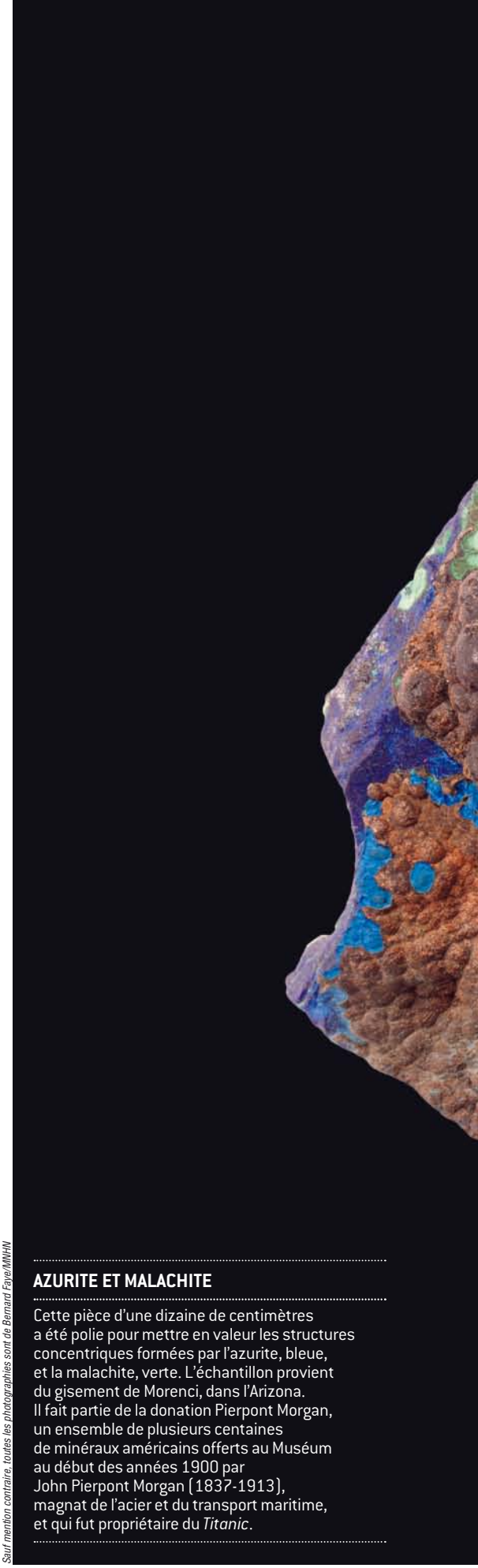
La Galerie de minéralogie du Muséum, à Paris, rouvre ses portes au public avec une exposition de plusieurs centaines de ses plus beaux spécimens. Aperçu sur quelques-uns de ces joyaux.

Maurice Mashaal

Parmi les plus importantes au monde, la collection de minéralogie du Muséum national d'histoire naturelle, à Paris, est riche de près de 130 000 spécimens. Le public va pouvoir en admirer certains des plus beaux : après une fermeture de dix ans pour travaux de rénovation, la Galerie de minéralogie a rouvert ses portes le 19 décembre 2014 en exposant environ 600 échantillons de minéraux et de météorites.

Le choix des pièces s'est fait sur des critères esthétiques, scientifiques ou historiques. Les visiteurs pourront contempler des minéraux bruts, des gemmes taillées ou non, une vingtaine de cristaux géants, des joyaux historiques tels que le Grand saphir de Louis XIV, des objets sculptés, des tables florentines... Un échantillonnage qui reflète la grande diversité de la collection de minéralogie, constituée et enrichie depuis près de quatre siècles grâce à des achats, des expéditions naturalistes, des dons ou des opérations de mécénat.

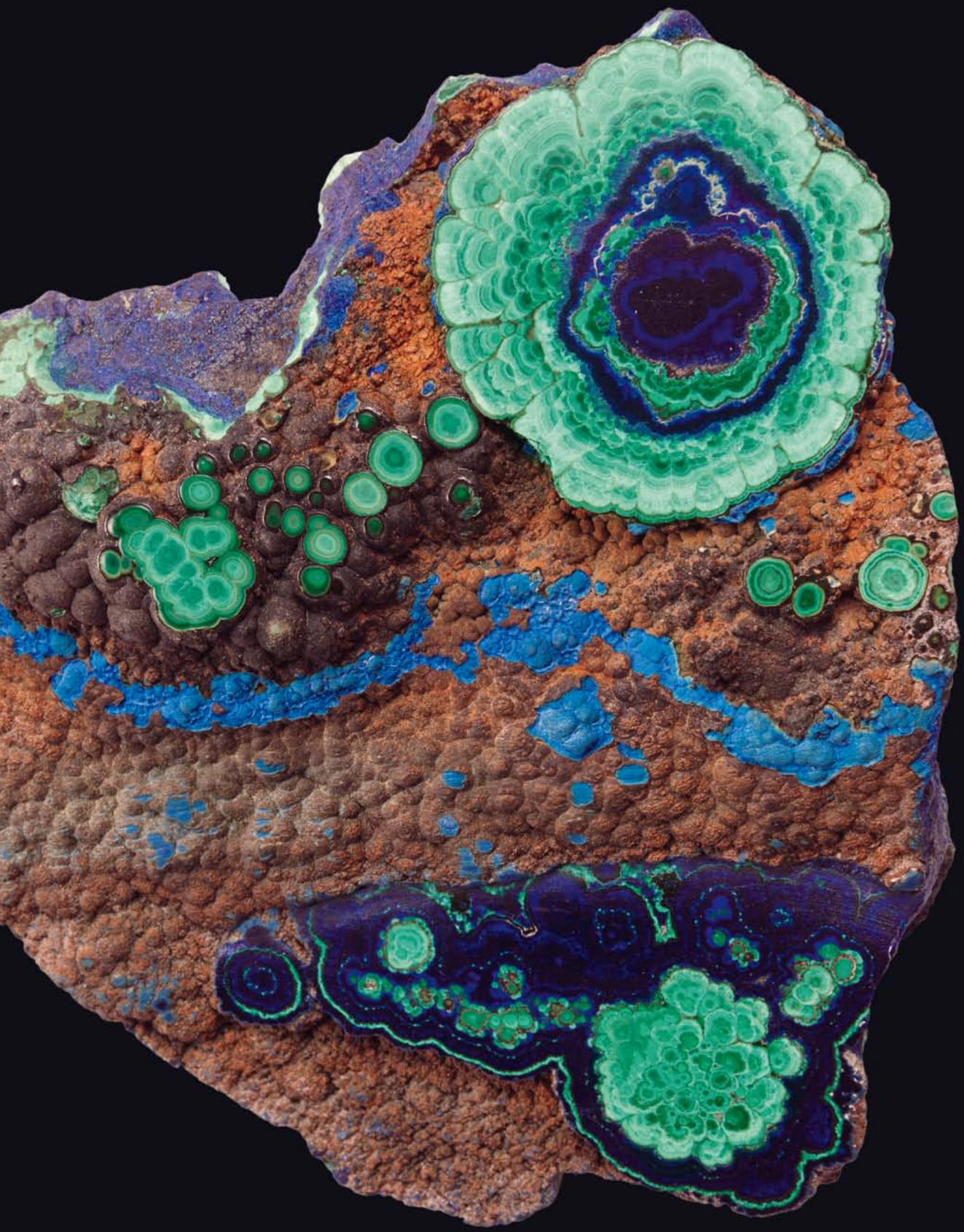
Cette collection et celles de géologie (quelque 334 000 spécimens de roches, 4 000 morceaux provenant de 1 500 météorites, un total de huit kilomètres de carottes de sédiments) sont conservées pour leur majeure partie dans la Galerie de minéralogie [et de géologie]. Ce bâtiment long de près de 200 mètres et datant des années 1830 est le premier, en France, à avoir été construit pour servir de musée. Sa réouverture au public n'est que partielle, l'espace de l'actuelle exposition n'occupant qu'une petite partie (250 mètres carrés) de la Galerie. Pour le reste, il faudra patienter encore quelques années ! ■



Sauf mention contraire, toutes les photographies sont de Bernard Faye/MNHN

AZURITE ET MALACHITE

Cette pièce d'une dizaine de centimètres a été polie pour mettre en valeur les structures concentriques formées par l'azurite, bleue, et la malachite, verte. L'échantillon provient du gisement de Morenci, dans l'Arizona. Il fait partie de la donation Pierpont Morgan, un ensemble de plusieurs centaines de minéraux américains offerts au Muséum au début des années 1900 par John Pierpont Morgan (1837-1913), magnat de l'acier et du transport maritime, et qui fut propriétaire du *Titanic*.

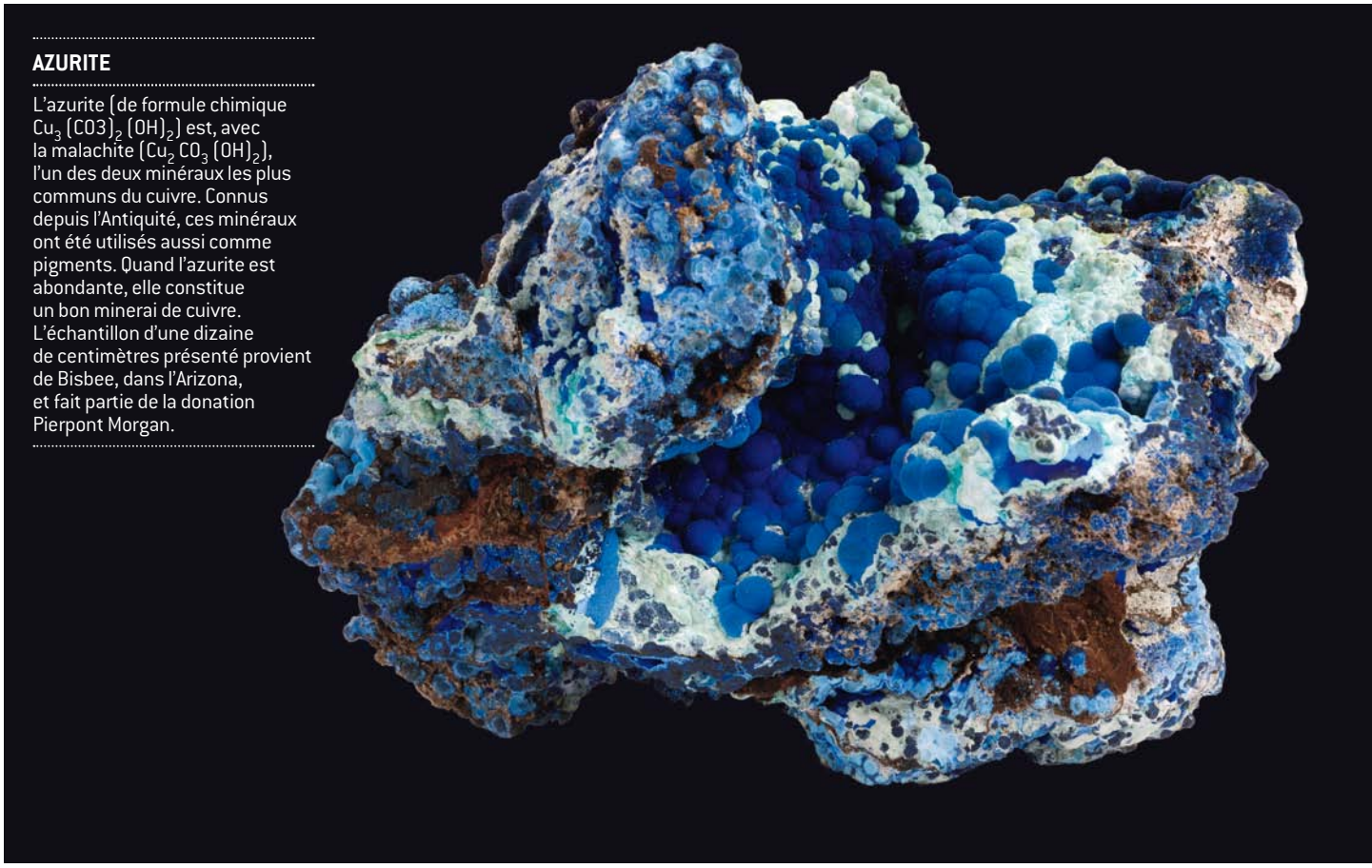


ELBAÏTE RUBELLITE

Cet échantillon d'elbaïte de variété rubellite est un minéral du groupe des silicates appartenant à la famille des tourmalines. D'autres variétés colorées de la même famille sont la verdelite (vert à vert foncé-bleu) et l'indicolite (bleue). La composition chimique de l'elbaïte est $Na(Al, Li)_3 Al_6(BO_3)_3 Si_6O_{18}(OH)_4$. La pièce présentée mesure 17 centimètres dans sa plus grande dimension et provient de Pala, en Californie (donation Pierpont Morgan).

AZURITE

L'azurite (de formule chimique $Cu_3(CO3)_2(OH)_2$) est, avec la malachite ($Cu_2CO_3(OH)_2$), l'un des deux minéraux les plus communs du cuivre. Connus depuis l'Antiquité, ces minéraux ont été utilisés aussi comme pigments. Quand l'azurite est abondante, elle constitue un bon minerai de cuivre. L'échantillon d'une dizaine de centimètres présenté provient de Bisbee, dans l'Arizona, et fait partie de la donation Pierpont Morgan.



RHODOCHROSITE

La rhodochrosite est un carbonate de manganèse ($MnCO_3$). Cet échantillon, qui mesure 41 centimètres dans sa plus grande dimension, est une section transversale de stalactite et provient de Capillitas, dans la province de Catamarca au Nord-Ouest de l'Argentine (pièce acquise par le Muséum grâce au mécénat du groupe *Total*).
En général, les stalactites sont constituées d'aragonite ($CaCO_3$), mais comme les fluides de ce gisement contiennent du manganèse, de la rhodochrosite a pu se former.
Les différences de teintes sont dues aux différences de concentration en manganèse.

ORPIMENT BRUN ORANGÉ ET CALCITE

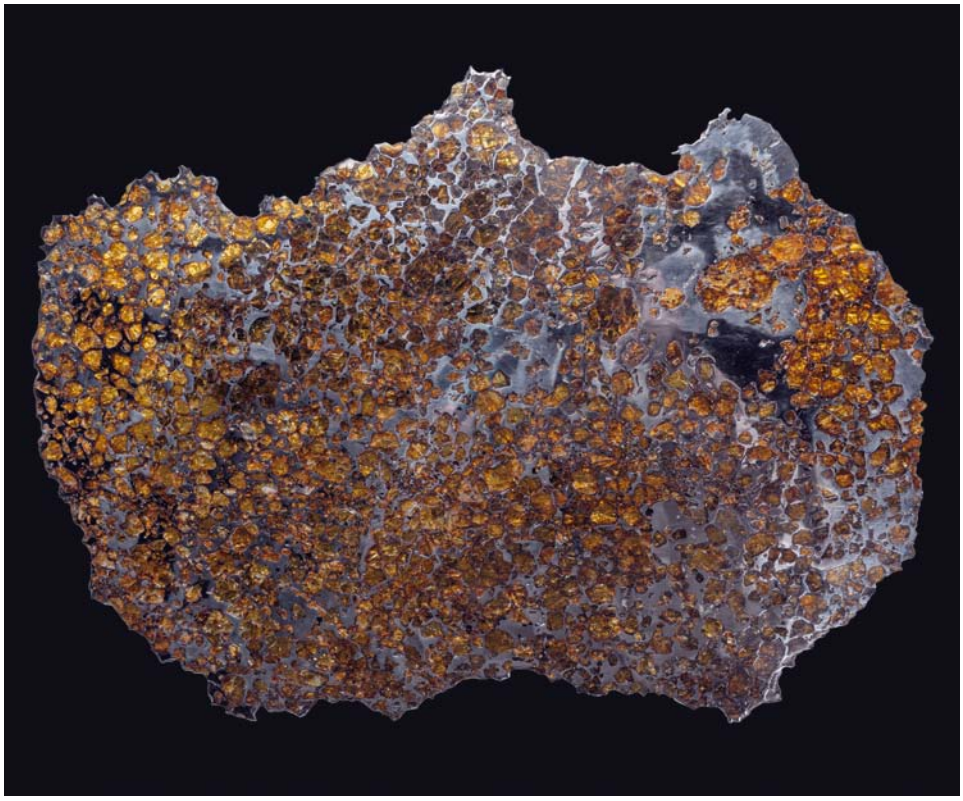
Dans cette pièce faisant plus de 15 centimètres, des cristaux d'orpiment se sont formés parmi des cristaux de calcite blanche. L'orpiment est un sulfure d'arsenic (As_2S_3) assez répandu, mais qui se présente rarement sous la forme de cristaux prismatiques. L'échantillon provient du gisement de Shimen, dans la province du Hunan, en Chine.

FOSSILES EN OPALE

Ces opales proviennent du gisement de Coober Pedy, dans le Sud de l'Australie. Il s'agit ici de fossiles de rostres de bélemnites, des céphalopodes marins disparus à la fin du Crétacé, il y a quelque 65 millions d'années. Longs d'une dizaine de centimètres, ces rostres inclus dans une gangue de calcaire se sont transformés en opales lors de la fossilisation. L'opale est un colloïde de silice hydratée ($SiO_2 \cdot n\,H_2O$). Sa structure cristalline est particulière, en partie amorphe, ce qui est à l'origine des irisations.

OR ENCHÂSSÉ DANS DU QUARTZ

Un minéral est une substance naturelle, formée généralement par un processus géologique, et qui est le plus souvent sous forme solide dans les conditions habituelles de température et pression. Il est caractérisé par sa composition chimique et sa structure cristalline (à l'échelle atomique). Lorsque le minéral est formé d'un seul élément chimique, on parle d'élément natif. C'est le cas de l'or dans cet échantillon collecté à Saint-Élie, en Guyane française.



TRANCHE DE MÉTÉORITE

Cette tranche de météorite pèse 1,26 kilogramme et mesure une quarantaine de centimètres. Elle provient de la météorite d'Imilac, trouvée en 1822 dans le désert chilien de l'Atacama et qui pesait 920 kilogrammes. Elle appartient à la famille des pallasites, météorites constituées de cristaux d'olivine (dont une variété est le péridot) inclus dans une matrice de fer-nickel. Les pallasites proviendraient de la limite entre le noyau et le manteau d'astéroïdes dotés d'une structure interne différenciée.

MONOCLE ET BINOCLE

L'agate est une variété de calcédoine, un minéral composé de silice. Elle présente souvent des bandes concentriques de couleurs différentes, déterminées par les diverses impuretés contenues dans la roche. Celle montrée ici est remarquable par les motifs qu'elle arbore sur ses deux faces.
Elle fait partie des quelque 2 000 belles pierres collectionnées à partir des années 1950 par l'écrivain français Roger Caillois (1913-1978), et dont une part notable est allée au Muséum par dation en 1988.

CALCITE

Cette calcite dite de Bellecroix provient de Fontainebleau, en région parisienne, et sa taille est de 22 centimètres. Son faciès globulaire, avec une multitude de petits cristaux enchevêtrés, est étonnant. La calcite est un carbonate de calcium ($CaCO_3$) et constitue le principal minéral des roches sédimentaires calcaires. C'est l'un des minéraux les plus répandus et elle présente des centaines de formes différentes, parfois colorées grâce aux impuretés ou inclusions d'autres minéraux. La calcite pure est transparente ; elle a notamment permis de découvrir le phénomène optique de double réfraction.

Trésors de la Terre, exposition à partir du 19 décembre 2014, Galerie de minéralogie, Muséum national d'histoire naturelle, Paris.

Collectif, **Trésors de la Terre - Galerie de minéralogie,** Artlys-MNHN, 2014.

Site Internet de la Galerie de minéralogie du Muséum : www.galeriedemineralogie.fr

Comment se protéger de Big Brother

Alex Pentland

À l'ère des données massives, nos vies entières se retrouvent sur Internet. Comment éviter qu'elles soient surveillées sans le moindre contrôle ? En suivant trois principes.

Pendant les premières décennies de son existence, l'Agence de sécurité américaine (NSA, ou *National Security Agency*) avait pour objectif principal de surveiller l'Union soviétique. Son ennemi était alors monolithique et bien défini. Elle se fondait surtout sur des écoutes téléphoniques, des avions espions et des microphones cachés.

Après les attaques du 11 septembre 2001, la situation a changé. Le principal ennemi de la NSA est devenu un réseau diffus de terroristes. Il pouvait être utile d'espionner n'importe qui. La nature même de l'espionnage a changé, avec la prolifération de nouveaux canaux de communication numériques. La croissance exponentielle des appareils mobiles connectés à Internet ne faisait que commencer. Dès lors, les vieux outils de la NSA se semblaient plus suffisants.

L'agence a réagi en adoptant une nouvelle stratégie : tout collecter. Selon Keith Alexander, le précédent directeur de la NSA, lorsqu'on cherche une aiguille dans une botte de foin, on a besoin de toute la botte. La NSA a d'abord collecté en masse des conversations téléphoniques, obtenant des enregistrements de presque toutes les personnes présentes sur le sol américain, puis elle a rassemblé des données sur le trafic Internet de presque tous les individus à l'échelle mondiale. En peu de temps, la NSA s'est mise à collecter toutes les deux heures une quantité de données équivalente à celle du recensement américain.

L'agence stockait toutes ces données dans ses propres locaux sécurisés, mais une telle concentration n'était pas sans conséquences. Les données personnelles de presque tous les individus du monde entier se trouvaient soudain à une touche de clavier de n'importe quel analyste de la NSA. En outre, le problème des fuites se posait de façon accrue.

Scandalisé par cette gigantesque collecte de l'ombre, Edward Snowden, alors consultant pour la NSA, a téléchargé des milliers de fichiers secrets depuis un serveur à Hawaï, s'est embarqué sur un vol pour Hong Kong et a remis les documents à la presse.

L'ESSENTIEL

- **Les données sur les individus sont essentielles aux gouvernements et aux industries, mais leur collecte peut donner lieu à des abus.**
- **Selon l'auteur, on éviterait ces abus si l'on appliquait quelques principes, notamment la répartition des données massives dans des centres séparés et la sécurisation des transmissions et du stockage.**
- **Les procédures doivent aussi être constamment adaptées pour suivre les évolutions techniques.**

Les gouvernements et les industries ont toujours eu besoin de rassembler des informations sur les individus, par exemple lors des recensements. Mais un saut qualitatif a été franchi avec la collecte de données sur des populations entières par une agence secrète, leur stockage dans des salles de serveurs clandestines et leur exploitation presque sans contrôle extérieur. Il n'est donc pas surprenant que les révélations d'E. Snowden aient déclenché un débat public intense.

Jusqu'ici, ce débat s'est surtout focalisé sur les dimensions morales et politiques du problème, tandis que les aspects techniques et structurels ont peu retenu l'attention. Pourtant, ils sont essentiels et permettraient de mettre en place certains garde-fous. En outre, en matière de collecte et d'utilisation des données massives (ou *big data*), les pratiques gouvernementales sont inadéquates. Ces pratiques, ainsi que leurs processus d'évaluation, doivent évoluer aussi vite que les techniques. Il n'existe pas de solution simple, mais on devrait appliquer quelques principes de base. Présentons-les.

PRINCIPE 1
Éparpiller la botte de foin

K. Alexander se trompait sur la recherche d'aiguilles dans une botte de foin. On n'a pas besoin de toute la botte, mais juste de la capacité d'en examiner n'importe quelle partie. Non seulement le stockage d'énormes quantités de données dans un même endroit n'est pas nécessaire, mais il présente un danger aussi bien pour les espions que pour les espionnés. Pour les gouvernements, cela rend les fuites dévastatrices plus probables. Pour les individus, cela crée un risque sans précédent de violation de la vie privée.

Les révélations d'E. Snowden ont montré qu'entre les mains du gouvernement, les données massives sont devenues bien trop concentrées. La NSA et les autres organisations gouvernementales devraient laisser les données en place, sous forme chiffrée et sous la surveillance de l'organisme qui a créé la base de données. En outre, il faudrait stocker séparément les différents types de données : les informations financières dans une base de données à tel endroit, les renseignements médicaux à tel autre endroit, etc. De façon générale, les informations sur les individus devraient être traitées à part. La NSA, ou toute autre entité ayant une raison légale de le faire, sera encore capable d'examiner n'importe quelle partie de cette vaste botte de foin. Elle ne pourra simplement plus stocker la botte entière dans un seul centre de serveurs.

Le plus simple est alors de stopper l'accumulation des données par les agences gouvernementales. Laissons les compagnies de télécommunication et d'Internet garder leurs enregistrements. S'empresser de détruire les centres de données de la NSA n'aurait pas une grande utilité, car leur contenu et les logiciels associés seront bientôt périmés.

La NSA n'abandonnera probablement pas ses activités de collecte de données sans une loi qui l'y oblige ou un ordre de l'exécutif. Pourtant, ce serait dans son intérêt, et les autorités semblent le savoir. En 2013, Ashton Carter, alors adjoint du Secrétaire de la Défense, a diagnostiqué : « L'échec [l'affaire Snowden] a pour origine deux pratiques que nous devons abolir [...]. Il y avait une énorme quantité d'informations concentrée en un endroit. C'est une erreur. » Et en second lieu, « un individu a reçu l'autorité pour

accéder à cette information et la déplacer. Ce n'aurait pas dû être le cas non plus. » Des bases de données chiffrées, réparties sur différents systèmes informatiques, auraient non seulement compliqué une fuite de ce type, mais elles protègeraient aussi contre des cyberattaques venues de l'extérieur. Une intrusion ne donnerait accès qu'à une partie de la base de données. Même des gouvernements autoritaires y trouveraient leur intérêt : la concentration des données faciliterait un piratage massif par des individus qui se seraient introduits dans un centre de stockage.

Répartir les données aiderait aussi à protéger la vie privée, parce que cela rend possible l'analyse des « schémas de communication » entre les bases de données et les opérateurs humains. Chaque fois que quelqu'un rechercherait un élément particulier ou établirait des statistiques, cette opération laisserait une signature caractéristique, composée d'un réseau de liens et de transmissions entre bases de données. On pourrait utiliser ces signatures, métadonnées à propos de métadonnées, pour surveiller les opérations réalisées.

Considérons l'analogie suivante : au sein d'une entreprise, quand les schémas de communication sont visibles (par exemple lorsque des lettres sont transmises d'un service à l'autre), les employés peuvent identifier ceux qui correspondent à des opérations normales, même si les opérations elles-mêmes (le contenu des lettres) leur demeurent cachées. Supposons que le service financier se mette à examiner une quantité anormale de données privées sur la santé des employés : la personne chargée de garder à jour ces informations peut s'en apercevoir et en demander la raison. De même, structurer les opérations liées aux données massives de façon à créer des métadonnées à propos de métadonnées rendrait la surveillance possible. Les sociétés de télécommunication accèderaient à une certaine traçabilité de leurs données. Des associations civiles indépendantes et la presse pourraient s'assurer que les agences gouvernementales ne vont pas trop loin. Avec les métadonnées sur les métadonnées, nous serions capables de faire à la NSA ce que la NSA fait aux autres.

L'AUTEUR

Alex PENTLAND est directeur du Laboratoire de dynamique humaine du MIT, aux États-Unis, et codirige les projets du Forum économique mondial en matière de *big data* et données personnelles.

© Shutterstock.com/360b

EDWARD SNOWDEN, ALORS CONSULTANT POUR LA NSA, a rendu public en 2013 le programme de surveillance de masse exercé par l'agence.

BIBLIOGRAPHIE

A. Pentland, **Social Physics : How Good Ideas Spread - The Lessons from a New Science,** Penguin Press, 2014.

Personal Data: The Emergence of a New Asset Class, World Economic Forum, 2011, www.weforum.org/reports/personal-dataemergence-new-asset-class

A. Pentland, **Orienter la société grâce aux données massives,** *Pour la Science* n° 443, nov. 2013.

PRINCIPE 2

Sécuriser les transmissions

L'élimination des grands centres de données de la NSA n'est qu'une des étapes vers le respect de la vie privée. Il importe aussi de sécuriser le stockage et la transmission des données, notamment *via* le chiffrement. Appliquer cette forme de protection est particulièrement urgent dans un monde où la cybercriminalité et les menaces de cyber-guerre se développent.

Chaque utilisateur de données personnelles – gouvernement, entreprise ou individu –, devrait suivre des règles de sécurité de base. Il faudrait que le partage de données ne soit autorisé qu'entre des systèmes ayant des niveaux de sécurité équivalents. Chaque opération devrait requérir une chaîne fiable de certificats d'identité, afin de savoir d'où viennent les données et où elles vont. Les métadonnées utilisées devraient être contrôlées et les entités qui s'en servent soumises à diverses vérifications, comme on le fait pour lutter contre la fraude touchant les cartes de crédit.

Un bon modèle est ce qu'on appelle un réseau de confiance. Un tel réseau garde la trace des autorisations accordées aux utilisateurs pour chaque opération sur les données, en prenant en compte un cadre légal qui spécifie ce qui peut ou ne peut pas être fait, ainsi que les conséquences d'une violation des autorisations. Grâce à cet historique, les réseaux de confiance peuvent être automatiquement audités afin de vérifier que les données ne sont pas utilisées de façon abusive.

Ces réseaux se sont révélés à la fois sûrs et robustes. Le plus connu est celui de la Société pour les télécommunications financières entre les banques à l'échelle mondiale (SWIFT, pour *Society for Worldwide Interbank Financial Telecommunication*), par lequel quelque 10 000 banques et autres organisations transfèrent de l'argent. Le réseau de SWIFT n'a jamais été piraté (pour autant que nous le sachions).

Lorsqu'on lui a demandé pourquoi il s'était attaqué aux banques, le cambrioleur Willie Sutton aurait répondu : « parce que c'est là que se trouve l'argent ». Aujourd'hui, l'argent se trouve dans le réseau de SWIFT,

La solution dans une décentralisation extrême ?

Si les pratiques de la NSA ont causé un scandale international, les agences de renseignement françaises ne sont pas en reste pour la surveillance téléphonique et électronique de grande envergure. Moins d'un mois après les révélations d'Edward Snowden, l'interception des communications privées en France, aux frontières de la légalité, était dénoncée par les médias.

Cette dérive résulte de la centralisation des données, comme l'explique Alex Pentland dans cet article, et du fait qu'il soit devenu trivial de les consulter et de les croiser. Au-delà des pratiques des agences de renseignement, l'ère des données massives est confrontée à des enjeux contradictoires : comment à la fois publier des données d'utilité publique (recensement, fréquentation du métro, géolocalisation pour le covoiturage, etc.) et protéger la vie privée des individus ?

Depuis près d'une dizaine d'années, l'équipe Systèmes d'information sécurisés et mobiles d'Inria (Institut national de recherche en informatique et en automatique), à Paris, dont je suis membre associé, travaille sur le projet PlugDB (pour *Plug Database*, littéralement base de données à brancher). Ce projet se fonde sur des principes proches de ceux présentés par A. Pentland, en particulier la décentralisation des données, tout en allant plus loin sur la sécurité et la confiance. L'élément central du dispositif est un petit appareil sécurisé connectable à un ordinateur. Il permet aux individus de stocker leurs données ou des liens sur ces données, et surtout d'en contrôler l'accès, le partage, la modification et la destruction.

C'est au sein même de ce dispositif hautement sécurisé que s'exécutent les applications de gestion de données, et non dans un serveur d'Internet ou sur un ordinateur. Il faudra alors que les concepteurs d'applications fournissent les logiciels nécessaires pour les faire fonctionner. Le dispositif est sécurisé même contre l'utilisateur : quand ce dernier souhaite utiliser un logiciel, il est assuré que c'est bien lui qui s'exécute, mais il ne peut ni voir ni modifier le code sous-jacent. Les concepteurs sont alors libres de publier ou non le code, pour des raisons de transparence ou de secret industriel.

Prenons l'exemple de l'application *Google Flu Trends*, qui permet de prévoir les épidémies de grippe. Même si *Google* garantit contractuellement l'anonymat des utilisateurs et explique n'avoir besoin que de données agrégées (par exemple le nombre de fois que certains mots clés apparaissent dans une zone géographique), il stocke en réalité de manière centralisée l'intégralité des requêtes posées, ainsi que différents paramètres liés à l'utilisateur (telle l'adresse IP). Et ce pendant plusieurs années ! Ces données sont à la merci d'un piratage et d'un usage abusif par *Google* ou par les États faisant pression sur l'entreprise.

Avec un instrument comme PlugDB, l'utilisateur n'a pas besoin de dévoiler ses données personnelles, dont il reste maître. Il peut choisir la précision de celles qui sont divulguées, surveiller les accès et leur fixer une date limite, etc. La confiance est permise par l'utilisation d'un système d'exploitation transparent (dont le code est librement consultable) et de matériel sécurisé, qui n'autorise pas la falsification des données, même par leur détenteur.

– Benjamin Nguyen
Institut national des sciences appliquées (INSA), Bourges

où des milliers de milliards de dollars transitent chaque jour. Grâce notamment à ses systèmes de contrôle de métadonnées et de vérification automatique, ce réseau de confiance repousse les cambrioleurs et assure un trajet fiable des fonds jusqu'à la destination souhaitée.

Autrefois, les réseaux de confiance étaient complexes et leur fonctionnement coûteux, mais la démocratisation des capacités de calcul les a rendus accessibles à de petites organisations, voire à des individus. En partenariat avec l'Institut de conception guidée par les données, à Boston, mon équipe de l'Institut de technologie du Massachusetts (MIT) a participé à la construction de centres de données personnelles ouverts, ou *open* PDS (pour *Personal Data Store*), une version grand public de ce type de système. À l'heure actuelle, nous les testons avec des partenaires industriels et gouvernementaux. L'idée est de permettre à tous un partage de données sensibles, notamment sanitaires et financières, avec un niveau de sécurité équivalent à celui de SWIFT. Quand les réseaux de confiance se répandront, il deviendra plus sûr d'échanger des données, dont l'enregistrement dans des architectures de stockage réparties et sécurisées protégera à la fois les individus et les organisations ; ainsi, les mauvaises utilisations des données massives devraient être évitées.

PRINCIPE 3

Toujours expérimenter

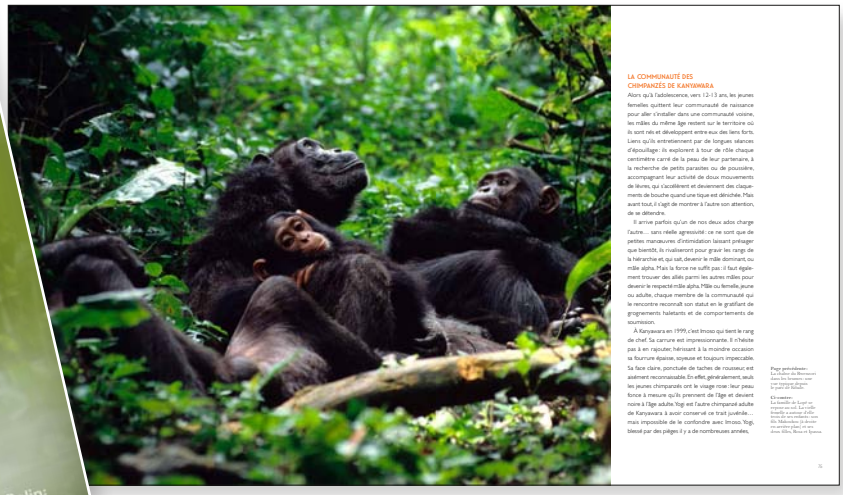
Le dernier principe, peut-être le plus important, est d'admettre que nous n'avons pas toutes les réponses et qu'il n'y a pas de solution définitive. Nous devons continuellement nous adapter. L'ère du numérique est totalement nouvelle, de sorte que nous ne pouvons pas nous contenter de méthodes classiques.

Sous la pression des autres pays, des citoyens et des entreprises du Web, la Maison Blanche a déjà proposé de limiter la surveillance exercée par la NSA. Dans un effort pour restaurer la confiance, les entreprises du Web cherchent à obtenir le droit de diffuser des informations sur les requêtes de l'agence – des métadonnées sur des métadonnées. En mai 2014, la Chambre des Représentants a voté une loi qui, bien que jugée insuffisante par de nombreux défenseurs de la vie privée, commençait à restreindre les collectes massives de données et à introduire un peu plus de transparence (cette loi a cependant été refusée par le Sénat en novembre).

Ces mesures vont dans la bonne direction, mais nous ne pourrons trouver que des solutions à court terme. Les techniques évoluent et les procédures gouvernementales doivent suivre le rythme. Finalement, le changement le plus important serait que nous décidions de conduire en continu des expériences et des tests à petite échelle, afin d'innover sans cesse et de trier ce qui fonctionne de ce qui ne fonctionne pas. ■

La sélection de livres pour la SCIENCE pour Noël

Sciences et images sont à l'honneur pour cette sélection spéciale Noël ! Découvrez la science comme vous ne l'avez jamais vue à travers de splendides photographies d'animaux, d'images du monde microscopique incroyables ou encore d'illustrations mathématiques uniques !



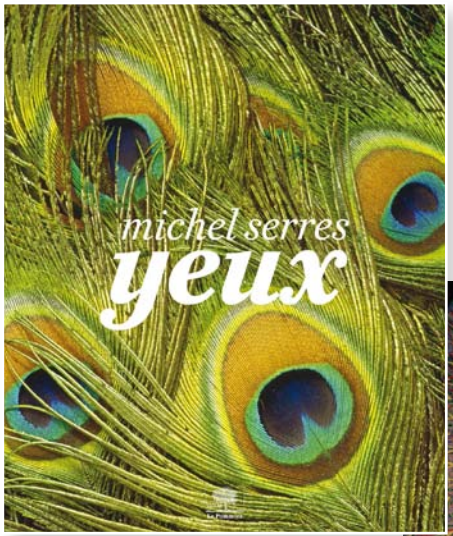
Les chimpanzés des Monts de la Lune

Sabrina Krief et Jean-Michel Krief, préface de Nicolas Hulot

Réf. 70118308

Imaginez-vous au cœur d'une forêt tropicale. À moins de dix mètres, des chimpanzés sauvages. Vous entendez leurs rires, leurs parties de jeu endiablées. Vous les voyez utiliser des outils, prendre soin de leurs petits, se soigner à l'aide de plantes. Voilà ce que vivent depuis plus de quinze ans Sabrina Krief, chercheuse au Muséum national d'Histoire naturelle, et Jean-Michel Krief, photographe. Ce beau livre est aussi le récit d'une aventure scientifique exceptionnelle.

Éditions Belin 2014 - 264 pages - 30 € - 978-2-7011-8308-4



Yeux

Michel Serres

Réf. 74650779

Comment voit-on ? Qu'est-ce que voir ? Être vu ? Quelles performances de vision peut-on rencontrer dans la nature ? Et jusqu'où l'homme pourra-t-il « voir » le monde ? Dans ce livre magnifique, Michel Serres explore, à la façon de variations, les capacités des yeux, de tous les yeux.

Éditions Le Pommier 2014 - 216 pages - 39 € - 978-2-7465-0779-1

En partenariat avec les éditeurs

Belin ÉDITEUR INDÉPENDANT DEPUIS 1777

Éditions Le Pommier

Pour commander ces ouvrages www.pourlascience.fr/librairie

ou en renvoyant le bon de commande ci-contre.

50 expériences pour épater vos amis à table

Jack Guichard et Guy Simonin

Réf. 74650544

Retournez votre verre de vin sans en perdre une goutte, transformez l'eau en vin, créez un nuage dans une bouteille, mettez une olive en lévitation ! Des expériences très faciles à réaliser et enrichies d'une explication simple et compréhensible des phénomènes scientifiques en jeu.

Éditions Le Pommier 2013
168 pages – 18,90 €
978-2-7465-0544-5

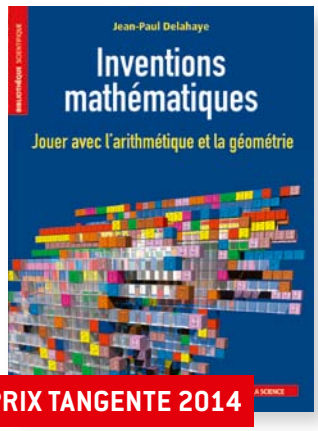
Micromonde

François Michel et Hervé Conge

Réf. 70117566

Partez à la découverte de l'architecture secrète du monde vivant et du monde minéral. Offrez-vous un voyage dans l'intimité de la nature, accompagné de commentaires joyeux.

Éditions Belin 2014 - 192 pages
23 € - 978-2-7011-7566-9



PRIX TANGENTE 2014

Inventions mathématiques

Jean-Paul Delahaye

Réf. 84245128

Dans ce livre, vous trouverez des figures paradoxales, des jeux classiques comme le Tangram et le cube de Rubik, des problèmes du quotidien tels le découpage d'une pizza ou l'accrochage d'un tableau, etc.

Éditions Belin-Pour la Science 2014
192 pages - 25 € - ISBN 978-2-8424-5128-8

Tous ces livres sont également disponibles en librairie.

BON DE COMMANDE

À retourner accompagné de votre règlement à :
Groupe Pour la Science • 628 avenue du Grain d'Or • 41350 Vineuil

❑ **Oui, je commande les livres** présentés dans la sélection de *Pour la Science*. Je reporte les titres, prix et références à 6 chiffres correspondant aux ouvrages choisis :

Titre	Réf.	Prix
		€
		€
		€
		€
		€
Frais de port (4,90 € France – 12 € étranger)	+	€
Total à régler	=	**€**

J'indique mes coordonnées :

Nom : _____

Prénom : _____

Adresse : _____

_____

C.P. : _____ Ville : _____

Pays : _____ Tél.* : _____ *facultatif

E-mail* : _____

@ _____

*pour recevoir la newsletter *Pour la Science* (à remplir en majuscules).

Je choisis mon mode de règlement :

❑ par chèque à l'ordre de *Pour la Science*

❑ par carte bancaire

Numéro _____

Date d'expiration _____

Cryptogramme _____

Signature obligatoire

POUR LA SCIENCE Belin ÉDITEUR INDÉPENDANT DEPUIS 1777 Le Pommier

En application de l'article 27 de la loi du 6 janvier 1978, les informations ci-dessus sont indispensables au traitement de votre commande. Elles peuvent donner lieu à l'exercice du droit d'accès et de rectification auprès du groupe *Pour la Science*. Par notre intermédiaire, vous pouvez être amené à recevoir des propositions d'organismes partenaires. **En cas de refus de votre part, merci de cocher la case ci-contre** ❑.

DPL447 Offre valable jusqu'au 31.01.2015, dans la limite des stocks disponibles.