PLAN STRATÉGIQUE 2026-2030 DE L'ASSOCIATION NATIONALE DE RÉGULATION DES DOMAINES ET DE L'INTERNET (ARDIN)

Document officiel — Version approuvée par le Conseil d'Administration Référence : ARDIN/PS/2026-2030/V1.0

MOT DU PRÉSIDENT

Le numérique n'est plus un secteur parmi d'autres : il est devenu l'infrastructure invisible sur laquelle repose la vie économique, sociale, démocratique et culturelle de nos nations. En quelques décennies, l'Internet a transformé nos façons de communiquer, de produire, d'apprendre et de gouverner. Cette transformation, portée par une accélération technologique sans précédent, ouvre des horizons considérables tout en soulevant des défis inédits en matière de sécurité, de souveraineté, de protection des droits fondamentaux et d'équité d'accès.

C'est dans ce contexte que l'Association Nationale de Régulation des Domaines et de l'Internet — l'ARDIN — assume, avec fierté et responsabilité, sa mission de vigie et d'architecte de la gouvernance numérique nationale. Depuis sa création, notre institution s'est attachée à construire un cadre de régulation équilibré, techniquement rigoureux et profondément humaniste, plaçant le citoyen au centre de chaque décision.

Le Plan Stratégique 2026-2030 que nous présentons aujourd'hui est le fruit d'une réflexion collective, menée avec l'ensemble de nos parties prenantes : institutions publiques, secteur privé, société civile, communauté technique et partenaires internationaux. Il définit la trajectoire ambitieuse que nous nous assignons pour les cinq prochaines années, articulée autour de sept axes stratégiques complémentaires : la gouvernance de l'Internet, la protection des données personnelles, la cybersécurité, le développement des compétences numériques, l'innovation et l'intelligence artificielle, la coopération internationale, et le renforcement institutionnel de l'ARDIN elle-même.

Notre vision est claire : faire de notre pays un acteur reconnu, souverain et responsable dans l'écosystème numérique mondial, au service du bien commun et du développement durable.

Je suis convaincu que ce plan stratégique, porté par des équipes engagées et des partenariats solides, permettra à l'ARDIN de franchir une nouvelle étape décisive dans son histoire et dans celle de la gouvernance numérique nationale.

Le Président du Conseil d'Administration *Association Nationale de Régulation des Domaines et de l'Internet*

MOT DU DIRECTEUR GÉNÉRAL

L'élaboration du Plan Stratégique 2026-2030 représente, pour les équipes de l'ARDIN, une étape fondatrice. Pour la première fois, notre institution se dote d'une feuille de route quinquennale intégrée, cohérente et mesurable, qui traduit notre vision en objectifs concrets, en programmes opérationnels et en indicateurs de performance vérifiables.

Le monde du numérique évolue à une vitesse vertigineuse. L'essor de l'intelligence artificielle générative, la prolifération des cybermenaces, la montée en puissance des réglementations sur la protection des données personnelles, la transition vers un Internet des objets omniprésent, et les enjeux croissants de souveraineté numérique redessinent en profondeur le paysage dans lequel nous opérons. Dans cet environnement mouvant, l'ARDIN doit faire preuve d'agilité stratégique, de rigueur technique et d'anticipation réglementaire.

Ce plan stratégique repose sur un diagnostic honnête de nos forces et de nos faiblesses, sur une analyse lucide des opportunités et des menaces de notre environnement, et sur une ambition mesurée mais résolument tournée vers l'excellence. Il s'articule autour de 7 axes stratégiques, 35 programmes prioritaires, et plus de 120 actions à mettre en œuvre sur la période 2026-2030, avec des échéances annuelles précises et des budgets prévisionnels indicatifs.

Nous avons également veillé à inscrire ce plan dans les cadres de référence internationaux les plus exigeants : les principes directeurs de l'ICANN pour la gestion des noms de domaine, le Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne, les recommandations de l'Union Internationale des Télécommunications (UIT) en matière de cybersécurité, et les Objectifs de Développement Durable (ODD) des Nations Unies.

Je tiens à remercier l'ensemble des collaborateurs de l'ARDIN, les membres du Conseil d'Administration, et les nombreux partenaires qui ont contribué à l'élaboration de ce document. C'est collectivement que nous relèverons les défis du numérique et construirons la confiance digitale de demain.

Le Directeur Général *Association Nationale de Régulation des Domaines et de l'Internet*

RÉSUMÉ EXÉCUTIF

Contexte et Enjeux

L'Association Nationale de Régulation des Domaines et de l'Internet (ARDIN) publie son premier Plan Stratégique quinquennal couvrant la période 2026-2030. Ce document de référence définit les orientations, les priorités et les moyens que l'institution entend mobiliser pour accomplir sa mission au service de la gouvernance numérique nationale et du développement d'un Internet sûr, ouvert et inclusif.

Le contexte dans lequel s'inscrit ce plan est marqué par une triple accélération : technologique (intelligence artificielle, informatique quantique, 5G/6G), réglementaire (RGPD, lois nationales sur le numérique, accords internationaux) et géopolitique (tensions autour de la souveraineté numérique, fragmentation potentielle de l'Internet). Ces dynamiques créent simultanément des opportunités majeures de développement et des risques nouveaux que l'ARDIN doit anticiper et maîtriser.

Vision 2030

« Un écosystème numérique national souverain, sécurisé, inclusif et innovant, au service des droits, du développement économique et du bien-être de tous les citoyens. »

Les 7 Axes Stratégiques

	Axe Stratégique	Priorité	Budget Indicatif (k€)
1	Gouvernance de l'Internet	Haute	200
2	Protection des données & conformité RGPD	Haute	100
3	Cybersécurité et confiance numérique	Critique	700
	TOTAL		**1 000**

Chiffres Clés 2026-2030

- **7 axes stratégiques**, **35 programmes prioritaires**, **120+ actions**
- **Budget prévisionnel global : 20 000 milliers d'euros** sur 5 ans
- **Taux de pénétration Internet cible : 85 %** de la population d'ici 2030 (contre 62 % en 2025)
- **Réduction des incidents cybersécurité majeure de 40 %** d'ici 2030
- **100 % des administrations publiques** conformes au cadre de protection des données d'ici 2028
- **50 000 citoyens formés** aux compétences numériques de base d'ici 2030
- **5 nouvelles conventions de coopération internationale** signées d'ici 2028

Mécanisme de Gouvernance

Le Plan Stratégique sera piloté par un **Comité de Pilotage Stratégique** présidé par le Directeur Général, avec des revues semestrielles, un rapport annuel public et une évaluation à mi-parcours prévue en 2028.

PARTIE I — PRÉSENTATION DE L'ARDIN

1.1 Historique et Genèse

L'Association Nationale de Régulation des Domaines et de l'Internet (ARDIN) a été fondée en réponse à l'émergence des défis posés par la révolution numérique dans notre pays. Créée par décret institutionnel, elle incarne la volonté des pouvoirs publics de doter la nation d'un organe de régulation spécialisé, indépendant et techniquement compétent, capable d'accompagner le développement de l'économie numérique tout en protégeant les droits fondamentaux des citoyens dans l'espace numérique.

Dès ses premières années d'existence, l'ARDIN s'est imposé comme l'interlocuteur de référence des acteurs nationaux et internationaux sur les questions relatives à la gouvernance de l'Internet, à la gestion des noms de domaine nationaux, à la cybersécurité et à la protection des données personnelles. Son action s'est progressivement structurée autour de quatre piliers fondateurs : **réguler, protéger, promouvoir et coopérer**.

L'institution a franchi des étapes décisives dans son développement institutionnel :

- **Phase de fondation** : Mise en place des structures de gouvernance, adoption des textes fondateurs, définition du cadre réglementaire initial pour la gestion du registre des noms de domaine nationaux ;
- **Phase de consolidation** : Développement des capacités techniques internes, établissement des premiers partenariats nationaux et internationaux, lancement des premières campagnes de sensibilisation ;
- **Phase d'expansion** : Extension des missions vers la cybersécurité et la protection des données personnelles, renforcement des équipes spécialisées, participation active aux forums de gouvernance de l'Internet aux niveaux régional et mondial ;
- **Phase actuelle (2026)** : Adoption du premier Plan Stratégique quinquennal, affirmation du positionnement de l'ARDIN comme pilier de la souveraineté numérique nationale.

1.2 Missions Institutionnelles

L'ARDIN est investi d'une mission d'intérêt général dont les composantes principales sont définies par ses textes constitutifs. Ces missions peuvent être regroupées en six domaines fondamentaux :

1.2.1 Gestion et Régulation des Noms de Domaine

L'ARDIN assure la gestion technique et administrative du registre des noms de domaine nationaux (ccTLD — Country Code Top-Level Domain). Elle définit les politiques d'enregistrement, garantit la stabilité et la sécurité du système de noms de domaine (DNS) national, et veille à la conformité des registraires accrédités avec les normes techniques et déontologiques en vigueur.

1.2.2 Protection des Données Personnelles

L'ARDIN exerce une fonction de contrôle et de conseil en matière de protection des données à caractère personnel. Elle instruit les plaintes des citoyens, délivre les autorisations de traitements sensibles, contrôle la conformité des organismes publics et privés, et prononce des sanctions administratives en cas de violation du cadre légal.

1.2.3 Cybersécurité et Confiance Numérique

L'ARDIN contribue à l'élaboration de la stratégie nationale de cybersécurité, coordonne les réponses aux incidents affectant les infrastructures numériques critiques, et développe des outils de sensibilisation et de formation à destination des acteurs publics, privés et des citoyens.

1.2.4 Gouvernance de l'Internet

L'ARDIN représente le pays dans les instances multilatérales de gouvernance de l'Internet (IGF, ICANN, UIT, forums régionaux) et contribue à l'élaboration des positions nationales sur les grandes questions de politique Internet au niveau mondial.

1.2.5 Sensibilisation et Éducation Numérique

L'ARDIN conduit des programmes d'éducation numérique à destination de l'ensemble de la population, avec une attention particulière pour les publics vulnérables, les jeunes, les seniors et les territoires sous-connectés.

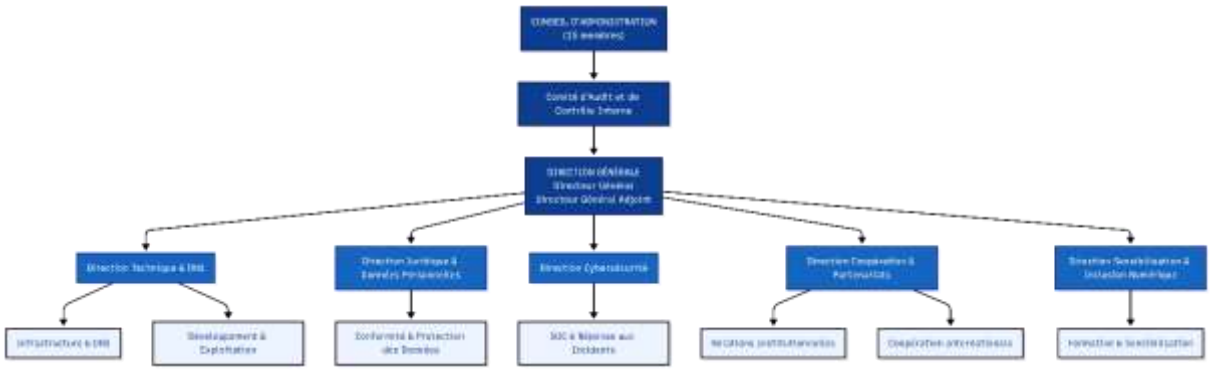
1.2.6 Certification et Confiance Numérique

L'ARDIN développe et gère un référentiel national de certification pour les prestataires de services numériques, notamment en matière d'hébergement, d'identité numérique et de signature électronique.

1.3 Organisation Institutionnelle

L'ARDIN est dotée d'une structure de gouvernance à cinq niveaux, garantissant l'indépendance de ses décisions, la représentativité de ses parties prenantes et l'efficacité de sa gestion opérationnelle.

Organigramme Fonctionnel



Composition du Conseil d'Administration

Catégorie de représentation	Nombre de membres
Représentants de l'État	4
Représentants du secteur privé	4
Représentants de la société civile	3
Experts techniques indépendants	2
Représentants des universités et centres de recherche	2
Total	**15**

1.4 Domaines d'Intervention

L'ARDIN intervient sur l'ensemble du spectre de la gouvernance numérique nationale, selon la cartographie suivante :

Domaine	Nature de l'intervention	Cadre légal de référence
Noms de domaine (ccTLD)	Régulation technique et administrative	Politiques ICANN, loi nationale
Protection des données	Contrôle, conseil, sanction	RGPD, loi nationale
Cybersécurité	Coordination, sensibilisation	Stratégie nationale cybersécurité
Gouvernance Internet	Représentation, participation	Forums IGF, ICANN

Domaine	Nature de l'intervention	Cadre légal de référence
Certification numérique	Accréditation, audit	eIDAS, normes ISO
Éducation numérique	Programmes, formation	Plan national d'inclusion
Innovation & IA	Veille, cadre éthique	Recommandations UNESCO, UE

PARTIE II — ANALYSE DU CONTEXTE NATIONAL ET INTERNATIONAL

2.1 La Transformation Numérique : Une Révolution Irréversible

La transformation numérique constitue sans doute la mutation sociotechnique la plus profonde depuis la révolution industrielle. À l'échelle mondiale, le nombre d'internautes dépasse désormais 5,5 milliards, soit plus de 68 % de la population mondiale (UIT, 2025). Dans notre pays, ce chiffre se situe autour de 62 %, avec d'importantes disparités territoriales entre les zones urbaines et rurales, ainsi qu'entre les différentes catégories socio-économiques de la population.

Cette transformation touche tous les secteurs : les administrations publiques développent leurs services en ligne, les entreprises numérisent leurs processus, les citoyens accomplissent leurs démarches du quotidien via des plateformes numériques. La pandémie de COVID-19 a considérablement accéléré ce mouvement, en imposant le télétravail, l'enseignement à distance et la télémédecine comme des modalités ordinaires de l'activité humaine.

Indicateurs clés de la transformation numérique nationale (2025) :

Indicateur	Valeur nationale	Moyenne régionale	Cible 2030
Taux de pénétration Internet	62 %	71 %	85 %
Taux d'équipement en smartphones	74 %	78 %	90 %
Part du e-commerce dans le commerce total	8,3 %	12,1 %	18 %
Services publics disponibles en ligne	43 %	67 %	95 %
Entreprises avec présence numérique	38 %	54 %	70 %
Couverture 4G du territoire	71 %	83 %	95 %

2.2 La Gouvernance de l'Internet : Enjeux Multilatéraux

La gouvernance de l'Internet demeure un champ de tensions et de négociations entre États, organisations internationales, acteurs privés et société civile. Le modèle multipartite défendu par des organisations telles que l'ICANN, l'Internet Society (ISOC) et le Forum sur la Gouvernance de l'Internet (IGF) se confronte à des velléités de fragmentation nationale de l'Internet (parfois qualifiées de « Splinternet ») portées par certains acteurs étatiques.

Les enjeux majeurs identifiés pour la période 2026-2030 incluent :

- **La stabilité du DNS mondial** et la protection contre les cyberattaques ciblant les infrastructures de nommage ;
- **La transition vers IPv6**, encore insuffisamment avancée dans de nombreux pays ;
- **L'encryptage de bout en bout** et les débats sur l'accès légal des autorités aux communications chiffrées ;
- **La neutralité du Net** et la lutte contre les pratiques de throttling discriminatoires ;
- **La gouvernance des plateformes numériques** et leurs obligations vis-à-vis du droit national ;
- **La souveraineté sur les données** et la localisation des données nationales sensibles.

2.3 Protection des Données Personnelles

L'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) de l'Union Européenne en 2018 a marqué un tournant décisif dans la régulation mondiale de la protection des données personnelles. Depuis lors, plus de 130 pays ont adopté ou renforcé leur législation nationale en la matière (UNCTAD, 2025).

Dans notre contexte national, la protection des données personnelles soulève plusieurs défis spécifiques :

- Le faible niveau de sensibilisation des citoyens à leurs droits numériques ;
- Les capacités limitées des entreprises, notamment les PME, à se mettre en conformité ;
- L'essor des services de cloud computing, souvent hébergés dans des juridictions étrangères ;
- La prolifération des applications mobiles collectant des données personnelles sans consentement éclairé ;
- La gestion des données sensibles dans le secteur de la santé, de l'éducation et des administrations publiques.

2.4 Cybersécurité : Une Menace en Constante Évolution

Le paysage des cybermenaces a connu une transformation radicale ces dernières années. Les attaques par ransomware, les campagnes de phishing sophistiquées, les attaques sur les chaînes d'approvisionnement logicielles (supply chain attacks), et les opérations d'influence numérique constituent désormais des menaces systémiques touchant aussi bien les gouvernements que les entreprises et les citoyens.

Évolution des incidents cybersécurité (estimation nationale 2023-2025) :

Type d'incident	2023	2024	2025 (est.)	Tendance
Ransomware	47	83	124	↑↑
Phishing	1 240	2 100	3 400	↑↑↑
Attaques DDoS	89	112	145	↑
Violations de données	23	41	67	↑↑
Fraude en ligne	3 200	4 800	6 500	↑↑↑
Incidents sur infrastructures critiques	8	14	19	↑↑

Le coût économique de la cybercriminalité est estimé à 6 000 milliards de dollars à l'échelle mondiale en 2025 (Cybersecurity Ventures). Pour notre pays, les estimations locales situent l'impact à environ 0,8 % du PIB annuel.

2.5 Intelligence Artificielle : Révolution et Régulation

L'intelligence artificielle représente probablement le défi réglementaire le plus complexe de la décennie. Les modèles de langage de grande taille (LLM), les systèmes de reconnaissance faciale, les algorithmes de décision automatisée et les outils de génération de contenu synthétique bouleversent les équilibres établis dans des domaines aussi variés que l'emploi, la justice, la santé, la démocratie et la créativité.

L'Union Européenne a adopté en 2024 le premier cadre réglementaire mondial sur l'IA (AI Act), qui établit une approche basée sur les risques et impose des obligations graduées aux développeurs et déployeurs de systèmes d'IA. Cette réglementation constitue un modèle de référence pour de nombreux pays, y compris le nôtre.

Pour l'ARDIN, l'IA soulève des questions transversales affectant l'ensemble de ses missions : les algorithmes de ciblage publicitaire et la protection des données, les deepfakes et la cybersécurité, les biais algorithmiques et l'équité numérique, la gouvernance des plateformes d'IA et la souveraineté nationale.

2.6 Inclusion Numérique

La fracture numérique demeure l'un des défis les plus préoccupants de la transformation numérique. Elle se manifeste selon plusieurs dimensions interdépendantes :

Fracture d'accès : Inégalités d'infrastructure (zones blanches, coût des équipements) ; **Fracture d'usage** : Manque de compétences numériques pour utiliser efficacement les outils disponibles ; **Fracture de qualité** : Disparités dans la qualité et la pertinence des usages numériques ; **Fracture de confiance** : Réticences à l'utilisation des services numériques, notamment chez les seniors et les populations vulnérables.

Profil de la fracture numérique nationale (2025) :

Groupe de population	Taux d'accès Internet	Taux de compétences numériques de base
18-34 ans	91 %	78 %
35-54 ans	75 %	58 %
55-74 ans	48 %	31 %
75 ans et plus	19 %	8 %
Zones urbaines	78 %	65 %
Zones rurales	41 %	28 %
Revenus élevés	94 %	82 %
Revenus faibles	37 %	22 %

2.7 Défis et Opportunités

Défis Majeurs

1. **Souveraineté numérique** : Dépendance aux technologies et infrastructures étrangères (hyperscalers, OS, semiconducteurs) ;
2. **Ressources humaines** : Pénurie mondiale de compétences en cybersécurité et en protection des données ;
3. **Capacités financières** : Budget contraint face à l'ampleur des besoins en infrastructure réglementaire ;
4. **Rythme législatif** : Difficulté à faire évoluer le cadre légal aussi rapidement que les technologies ;
5. **Coopération multipartite** : Complexité de la coordination entre acteurs publics, privés et société civile ;
6. **Désinformation** : Propagation rapide des fausses informations via les réseaux sociaux numériques.

Opportunités Stratégiques

1. **Agenda numérique continental** : Dynamique régionale favorable à l'harmonisation réglementaire ;
2. **Financements internationaux** : Disponibilité de fonds dédiés à la gouvernance numérique et à la cybersécurité (UE, UIT, Banque Mondiale) ;
3. **Économie numérique** : Potentiel de croissance économique lié à la numérisation (estimé à +2,3 % de PIB d'ici 2030) ;
4. **Partenariats académiques** : Développement d'une recherche nationale en cybersécurité et gouvernance numérique ;
5. **Initiatives citoyennes** : Montée en puissance des mouvements de défense des droits numériques.

PARTIE III — DIAGNOSTIC STRATÉGIQUE (ANALYSE SWOT)

3.1 Matrice SWOT de l'ARDIN

FORCES (Strengths)

#	Force identifiée	Niveau d'impact
F1	Légitimité institutionnelle reconnue et ancrage légal solide	Élevé
F2	Expertise technique avérée en gestion du DNS national et des noms de domaine	Élevé
F3	Équipes pluridisciplinaires (juristes, ingénieurs, experts en politique numérique)	Moyen

#	Force identifiée	Niveau d'impact
F4	Réseau de partenaires nationaux et internationaux établi	Élevé
F5	Participation active aux forums de gouvernance de l'Internet (IGF, ICANN)	Moyen
F6	Infrastructure technique opérationnelle pour la gestion du ccTLD national	Élevé
F7	Indépendance institutionnelle garantie par les textes fondateurs	Élevé
F8	Expérience dans la conduite de campagnes de sensibilisation	Moyen

FAIBLESSES (Weaknesses)

#	Faiblesse identifiée	Niveau d'impact
W1	Ressources financières insuffisantes au regard des missions	Élevé
W2	Effectifs limités face à l'étendue du champ d'intervention	Élevé
W3	Notoriété insuffisante auprès du grand public	Moyen
W4	Outils de monitoring et de veille technologique à moderniser	Moyen
W5	Capacités limitées en matière de cybersécurité opérationnelle	Élevé
W6	Absence de cadre formel d'évaluation de l'impact des interventions	Moyen
W7	Dépendance à des financements publics susceptibles d'arbitrages budgétaires	Élevé
W8	Couverture géographique nationale insuffisante (concentration urbaine)	Moyen

OPPORTUNITÉS (Opportunities)

#	Opportunité identifiée	Probabilité	Impact
O1	Croissance continue du marché numérique national	Haute	Élevé
O2	Disponibilité de financements internationaux (UE, UIT, Banque Mondiale)	Haute	Élevé
O3	Harmonisation réglementaire régionale (RGPD, AI Act, NIS2)	Haute	Élevé
O4	Demande croissante des entreprises pour des certifications de conformité	Haute	Moyen
O5	Intérêt gouvernemental pour la souveraineté numérique	Haute	Élevé
O6	Développement de l'Internet des objets et nouvelles juridictions à réguler	Moyenne	Élevé
O7	Essor de la recherche académique nationale en sécurité numérique	Moyenne	Moyen
O8	Modèles de coopération Sud-Sud dans la gouvernance Internet	Haute	Moyen

MENACES (Threats)

#	Menace identifiée	Probabilité	Impact
T1	Sophistication croissante des cyberattaques	Très haute	Critique
T2	Tentatives de fragmentation de l'Internet mondial	Moyenne	Élevé
T3	Non-conformité des acteurs privés malgré la réglementation	Haute	Élevé
T4	Désinformation numérique et manipulation de l'information	Très haute	Élevé

#	Menace identifiée	Probabilité	Impact
T5	Évolutions technologiques (IA, quantique) dépassant le cadre légal existant	Haute	Élevé
T6	Compétition accrue pour les talents en cybersécurité et droit numérique	Haute	Moyen
T7	Instabilité budgétaire liée aux contraintes économiques nationales	Moyenne	Élevé
T8	Dépendance aux fournisseurs étrangers pour les infrastructures critiques	Haute	Élevé

3.2 Orientations Stratégiques issues du SWOT

Orientation	Type (SWOT)	Description
Capitaliser sur la légitimité pour mener des projets de certification	F1 × O4	Développer un référentiel national de certification
Saisir les financements internationaux pour combler les lacunes de capacité	W1 × O2	Programmes de mobilisation de ressources externes
Renforcer l'expertise cyber pour contrer les menaces croissantes	W5 × T1	Plan de renforcement des capacités cybersécurité
Positionner l'ARDIN comme référence sur l'IA éthique	F3 × O3	Programme AI Governance & Ethics
Développer la présence territoriale pour lutter contre la fracture numérique	W8 × O1	Programme d'antennes régionales

---

PARTIE IV — VISION, MISSION ET VALEURS

4.1 Vision 2030

« Un écosystème numérique national souverain, sécurisé, inclusif et innovant, dans lequel chaque citoyen, chaque entreprise et chaque institution peut interagir en ligne avec confiance, en jouissant pleinement de ses droits numériques fondamentaux. »

Cette vision repose sur quatre piliers indissociables :

- **Souverain** : Un Internet dont la gouvernance respecte les intérêts et les valeurs nationales, sans compromettre son caractère universel et ouvert ;
- **Sécurisé** : Un espace numérique protégé contre les cybermenaces, les abus et les violations de données ;
- **Inclusif** : Un Internet accessible à tous, sans discrimination géographique, sociale, économique ou générationnelle ;
- **Innovant** : Un écosystème numérique qui stimule la créativité, l'entrepreneuriat et le développement économique.

4.2 Mission Institutionnelle

« L'ARDIN régule, protège et promeut l'écosystème numérique national dans l'intérêt général, en garantissant la stabilité des infrastructures Internet, la protection des données personnelles, la cybersécurité, et l'accès équitable de tous les citoyens aux opportunités du numérique. »

4.3 Valeurs Institutionnelles

L'ARDIN fonde l'ensemble de ses actions sur sept valeurs fondamentales qui guident ses décisions, ses relations avec ses partenaires et sa culture organisationnelle.

Valeur	Définition opérationnelle
Indépendance	Exercer nos missions sans influence politique, commerciale ou idéologique indue, au service exclusif de l'intérêt général
Excellence technique	Maintenir le plus haut niveau de compétence dans tous nos domaines d'intervention, en investissant continuellement dans la formation et la veille technologique
Transparence	Rendre compte publiquement de nos activités, de nos décisions et de l'utilisation de nos ressources, dans une logique de redevabilité démocratique
Innovation	Anticiper les évolutions technologiques et adapter proactivement notre cadre réglementaire, sans jamais courir derrière les transformations en cours
Inclusion	Garantir que notre action bénéficie à l'ensemble de la société, avec une attention particulière pour les populations les plus vulnérables et les plus éloignées du numérique
Coopération	Construire des partenariats durables et mutuellement bénéfiques avec tous les acteurs de l'écosystème numérique, aux niveaux national, régional et international
Intégrité	Exercer nos missions avec probité, éthique et rigueur déontologique, en plaçant les droits des citoyens au centre de toutes nos décisions

---

PARTIE V — AXES STRATÉGIQUES 2026-2030

AXE STRATÉGIQUE 1 : GOUVERNANCE DE L'INTERNET

1.1 Contexte

La gouvernance de l'Internet couvre l'ensemble des règles, normes, politiques et pratiques qui définissent le cadre de fonctionnement de l'Internet, depuis la couche technique (protocoles, DNS, adressage IP) jusqu'aux couches applicatives et de contenu. Pour une organisation comme l'ARDIN, la gouvernance de l'Internet constitue la mission fondatrice et la pierre angulaire de son existence institutionnelle.

À l'horizon 2026-2030, plusieurs évolutions majeures marqueront le paysage de la gouvernance Internet : la transition vers l'IPv6, le déploiement généralisé du DNSSEC pour sécuriser les échanges DNS, l'essor des nouvelles extensions de noms de domaine (new gTLDs), et les débats croissants sur la gouvernance des plateformes numériques dominant l'espace informationnel mondial.

1.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS1.1	Assurer la stabilité, la sécurité et la résilience du ccTLD national	2026-2030
OS1.2	Atteindre 100 % de déploiement DNSSEC sur le ccTLD national	2027
OS1.3	Porter le taux de pénétration IPv6 à 60 % des connexions nationales	2029
OS1.4	Renforcer la représentation nationale dans les instances de gouvernance Internet	2026-2030
OS1.5	Développer un cadre national de politique Internet cohérent et actualisé	2027

1.3 Programmes Prioritaires

Programme 1.A — Excellence DNS Modernisation et renforcement de l'infrastructure DNS nationale, déploiement intégral du DNSSEC, mise en place d'un système de surveillance en temps réel et développement d'un plan de continuité d'activité pour le ccTLD.

Programme 1.B — Transition IPv6 Élaboration et mise en œuvre d'un plan national de transition IPv6, sensibilisation des opérateurs télécoms et FAI, accompagnement technique des administrations publiques et des grandes entreprises.

Programme 1.C — Politique Internet Nationale Élaboration d'un Livre Blanc sur la Politique Internet Nationale, organisation d'un Forum National de Gouvernance de l'Internet (FNGI) annuel, et développement d'un processus multipartite de consultation.

Programme 1.D — Représentation Internationale Renforcement de la présence nationale à l'ICANN (GNSO, ccNSO, GAC), à l'IGF et dans les forums régionaux de gouvernance Internet, formation d'une délégation nationale compétente et représentative.

1.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A1.1	Audit complet de l'infrastructure DNS nationale	Direction Technique	T1 2026
A1.2	Déploiement DNSSEC sur 100 % des zones ccTLD	Direction Technique	T4 2026
A1.3	Publication de la Politique de Nommage révisée	Direction Juridique	T2 2026
A1.4	Lancement du plan national IPv6	Direction Technique	T3 2026
A1.5	Organisation du 1er Forum National de Gouvernance Internet	Direction Générale	T4 2026
A1.6	Accréditation de 5 nouveaux registraires ccTLD	Direction Technique	T2 2027
A1.7	Mise en place d'un système de résolution de litiges en ligne	Direction Juridique	T3 2027
A1.8	Publication du Livre Blanc sur la Politique Internet	Direction Générale	T1 2028
A1.9	Atteindre 50 % de déploiement IPv6	Direction Technique	T4 2028
A1.10	Révision quinquennale de la politique de nommage	Direction Juridique	T2 2030

1.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Taux de disponibilité du ccTLD (SLA)	99,5 %	99,9 %	99,99 %
Taux de déploiement DNSSEC	45 %	100 %	100 %
Nombre de noms de domaine ccTLD enregistrés	85 000	120 000	200 000
Taux d'adoption IPv6	12 %	35 %	60 %
Nombre de registraires accrédités	18	28	40
Délai moyen de résolution des litiges DNS	45 jours	30 jours	20 jours
Participation aux instances ICANN/IGF	2 événements/an	5 événements/an	8 événements/an

---

AXE STRATÉGIQUE 2 : PROTECTION DES DONNÉES PERSONNELLES ET CONFORMITÉ

2.1 Contexte

La protection des données personnelles est devenue un enjeu central de la gouvernance numérique mondiale. Dans notre contexte national, le cadre légal en matière de protection des données personnelles est en cours de modernisation pour s'aligner sur les meilleures pratiques internationales, notamment le RGPD européen. L'ARDIN est appelée à jouer un rôle pivot dans la mise en œuvre effective de ce cadre, en agissant simultanément comme régulateur, conseil et promoteur des droits numériques des citoyens.

La conformité au cadre de protection des données représente un défi majeur pour les organisations nationales, notamment les PME disposant de ressources limitées pour mettre en place les structures et processus requis.

2.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS2.1	Renforcer le cadre légal national de protection des données personnelles	2026-2027
OS2.2	Atteindre 100 % de conformité des administrations publiques	2028
OS2.3	Développer une culture de protection des données dans le secteur privé	2026-2030
OS2.4	Renforcer les droits des citoyens et les mécanismes de recours	2026-2030
OS2.5	Développer les capacités de contrôle et de sanction de l'ARDIN	2026-2028

2.3 Programmes Prioritaires

Programme 2.A — Cadre Légal et Réglementaire Révision et modernisation de la loi nationale sur la protection des données, alignement avec le RGPD, définition du régime de sanction, et publication de guides pratiques sectoriels.

Programme 2.B — Conformité des Acteurs Publics Plan d'accompagnement des administrations centrales et locales vers la conformité, désignation et formation des Délégués à la Protection des Données (DPO) publics, audits de conformité réguliers.

Programme 2.C — Accompagnement des Entreprises Programme d'accompagnement des PME vers la conformité, développement d'outils en ligne d'autoévaluation, création d'un label national de confiance numérique.

Programme 2.D — Droits des Citoyens Plateforme en ligne de traitement des plaintes, campagnes d'information sur les droits numériques, programme d'éducation à la vie privée en ligne.

2.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A2.1	Révision de la loi nationale sur la protection des données	Direction Juridique	T2 2026
A2.2	Publication du guide DPO pour le secteur public	Direction Juridique	T3 2026
A2.3	Lancement de la plateforme de dépôt de plaintes en ligne	Direction Technique	T4 2026
A2.4	Formation de 200 DPO publics et privés	Direction Juridique	T1-T4 2027
A2.5	Réalisation de 50 audits de conformité d'administrations publiques	Direction Juridique	T2 2027 - T4 2028
A2.6	Lancement du label national "Confiance Numérique"	Direction Générale	T3 2027
A2.7	Publication du référentiel de certification RGPD national	Direction Juridique	T1 2028
A2.8	Mise en place du registre national des traitements	Direction Technique	T2 2028
A2.9	Campagne nationale "Mes droits numériques"	Dir. Sensibilisation	2026-2030 (annuel)
A2.10	Bilan quinquennal de conformité	Direction Juridique	T4 2030

2.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
% d'administrations publiques conformes	23 %	65 %	100 %
Nombre de DPO formés et certifiés	45	300	800
Nombre de plaintes reçues et traitées/an	180	400	700
Délai moyen de traitement des plaintes	90 jours	60 jours	45 jours
% d'entreprises du CAC national avec DPO désigné	31 %	70 %	100 %
Nombre de labels "Confiance Numérique" délivrés	0	50	300

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Montant des sanctions prononcées (k€)	120	500	1 500
Taux de sensibilisation citoyenne aux droits numériques	18 %	40 %	65 %

AXE STRATÉGIQUE 3 : CYBERSÉCURITÉ ET CONFIANCE NUMÉRIQUE

3.1 Contexte

La cybersécurité représente le défi le plus urgent et le plus critique de l'ère numérique. Les incidents de cybersécurité affectent désormais toutes les catégories d'acteurs, des infrastructures critiques nationales aux PME, en passant par les particuliers. La sophistication croissante des attaquants, l'automatisation des outils malveillants par l'IA, et la dépendance accrue des sociétés aux systèmes numériques créent un contexte de risque systémique que l'ARDIN doit contribuer à maîtriser.

L'ARDIN n'est pas le seul acteur national de la cybersécurité — elle intervient en coordination avec les agences nationales de sécurité, les opérateurs d'infrastructures critiques et les organismes sectoriels — mais elle joue un rôle central dans la sensibilisation, la coordination interinstitutionnelle et le développement des capacités.

3.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS3.1	Réduire de 40 % le nombre d'incidents cybersécurité majeurs d'ici 2030	2030
OS3.2	Développer un centre national de veille et d'alerte cybersécurité	2027
OS3.3	Mettre en place un cadre national de certification en cybersécurité	2028
OS3.4	Renforcer la résilience des infrastructures numériques critiques	2026-2030
OS3.5	Développer une culture nationale de cybersécurité	2026-2030

3.3 Programmes Prioritaires

Programme 3.A — Centre de Veille et d'Alerte (CERT-ARDIN) Création et opérationnalisation d'un Computer Emergency Response Team (CERT) national coordonné par l'ARDIN, en charge de la détection des incidents, de l'alerte précoce et de la coordination des réponses.

Programme 3.B — Protection des Infrastructures Critiques Cartographie des infrastructures numériques critiques nationales, développement de standards de sécurité sectoriels, exercices de simulation de crise cyber annuels.

Programme 3.C — Certification Cybersécurité Développement d'un référentiel national de certification pour les prestataires de services de cybersécurité, création d'un label de sécurité numérique pour les produits et services digitaux.

Programme 3.D — Sensibilisation Cybersécurité Programme national de sensibilisation "CyberSafe", formation des agents publics à la cyberhygiène, campagnes ciblées pour les PME et les citoyens.

Programme 3.E — Lutte contre la Cybercriminalité Renforcement de la coopération avec les services de police et de justice, développement de capacités de forensic numérique, participation aux réseaux internationaux de lutte contre la cybercriminalité.

3.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A3.1	Création du CERT-ARDIN (équipe, infrastructure, procédures)	Dir. Cybersécurité	T2 2026
A3.2	Cartographie des infrastructures numériques critiques	Dir. Cybersécurité	T3 2026
A3.3	Publication du guide de cyberhygiène pour les PME	Dir. Cybersécurité	T4 2026
A3.4	Premier exercice national de simulation de crise cyber	Dir. Cybersécurité	T2 2027
A3.5	Lancement du programme "CyberSafe" pour les citoyens	Dir. Sensibilisation	T3 2027

Code	Action	Responsable	Échéance
A3.6	Déploiement d'une plateforme nationale de signalement cyber	Dir. Technique	T4 2027
A3.7	Publication du référentiel national de certification cyber	Dir. Cybersécurité	T1 2028
A3.8	Formation de 500 agents publics à la cyberhygiène	Dir. Sensibilisation	2027-2028
A3.9	Intégration dans le réseau FIRST (international CERTs)	Dir. Coopération	T3 2027
A3.10	Création d'un observatoire national des cybermenaces	Dir. Cybersécurité	T2 2029
A3.11	Publication du rapport annuel sur la cybersécurité nationale	Dir. Générale	2026-2030 (annuel)

3.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Réduction des incidents majeurs (%)	-	-20 %	-40 %
Délai moyen de détection d'un incident	72 heures	24 heures	8 heures
Nombre d'alertes émises par le CERT	0	50/an	200/an
% d'administrations ayant réalisé un audit cyber	8 %	40 %	80 %
Nombre de prestataires certifiés cybersécurité	0	20	80
Taux de sensibilisation des PME à la cybersécurité	12 %	35 %	60 %
Nombre d'exercices de crise organisés/an	0	1	3
Budget cybersécurité moyen des administrations/PIB	0,03 %	0,06 %	0,1 %

AXE STRATÉGIQUE 4 : DÉVELOPPEMENT DES COMPÉTENCES NUMÉRIQUES

4.1 Contexte

Le développement des compétences numériques constitue un prérequis indispensable à l'inclusion numérique et à la pleine participation des citoyens à l'économie et à la société numériques. Sans compétences adaptées, l'accès aux infrastructures ne suffit pas à réduire la fracture numérique.

L'ARDIN considère que son rôle en matière d'éducation et de formation numérique va au-delà de la simple sensibilisation : il s'agit de contribuer à la construction d'une culture numérique nationale, à tous les niveaux d'éducation et pour toutes les catégories de population.

4.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS4.1	Former 50 000 citoyens aux compétences numériques de base d'ici 2030	2030
OS4.2	Développer un référentiel national de compétences numériques	2027
OS4.3	Intégrer la culture numérique dans les programmes scolaires	2028
OS4.4	Réduire la fracture numérique de genre, générationnelle et géographique	2026-2030
OS4.5	Développer des filières de formation spécialisées en cybersécurité et IA	2027-2030

4.3 Programmes Prioritaires

Programme 4.A — DigiCompétences Développement d'un référentiel national de compétences numériques en cinq niveaux (de la sensibilisation à l'expertise), aligné sur le cadre européen DigComp 2.2.

Programme 4.B — DigitalInclusion+ Programme de formation itinérant à destination des populations les plus éloignées du numérique : seniors, zones rurales, personnes en situation de précarité. Déploiement de "bus du numérique" et de centres numériques de proximité.

Programme 4.C — EduNum Partenariat avec le ministère de l'Éducation nationale pour intégrer l'éducation au numérique dans les programmes scolaires de la maternelle au lycée.

Programme 4.D — NumPro Programme de formation aux métiers du numérique pour les demandeurs d'emploi et les travailleurs en reconversion, en partenariat avec les centres de formation professionnelle.

4.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A4.1	Publication du Référentiel National de Compétences Numériques	Dir. Sensibilisation	T2 2026
A4.2	Lancement de la plateforme e-learning ARDIN	Dir. Technique	T3 2026
A4.3	Déploiement de 10 centres numériques de proximité	Dir. Sensibilisation	T4 2026 - T4 2027
A4.4	Signature du partenariat avec le Ministère de l'Éducation	Dir. Générale	T1 2027
A4.5	Formation de 1 000 formateurs au numérique	Dir. Sensibilisation	T2-T4 2027
A4.6	Lancement du programme "Seniors et Numérique"	Dir. Sensibilisation	T3 2027
A4.7	Intégration de l'éducation numérique dans 200 écoles	Dir. Sensibilisation	T2 2028
A4.8	Lancement de 5 filières de formation en cybersécurité	Dir. Coopération	T3 2028
A4.9	Extension à 30 centres numériques de proximité	Dir. Sensibilisation	T4 2028
A4.10	Bilan et ajustement du programme DigiCompétences	Dir. Sensibilisation	T2 2029

4.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Nombre de citoyens formés (cumulé)	-	15 000	50 000
Nombre de centres numériques de proximité	2	15	30
Taux de compétences numériques de base (pop. +15 ans)	41 %	55 %	70 %
Nombre d'écoles intégrant l'éducation numérique	45	300	800
Nombre de formateurs certifiés au numérique	80	500	1 500
Part des femmes dans les formations numériques	32 %	45 %	50 %
Taux de satisfaction des bénéficiaires (formations)	-	80 %	90 %
Nombre d'apprenants sur la plateforme e-learning	0	8 000	30 000

AXE STRATÉGIQUE 5 : INNOVATION NUMÉRIQUE ET INTELLIGENCE ARTIFICIELLE

5.1 Contexte

L'intelligence artificielle et l'innovation numérique constituent à la fois une formidable opportunité de développement et un défi réglementaire sans précédent. L'ARDIN doit se positionner comme un acteur de référence sur les enjeux éthiques, juridiques et techniques liés à l'IA, tout en favorisant un environnement propice à l'innovation responsable.

L'adoption de l'AI Act européen en 2024 a établi un cadre réglementaire de référence mondial basé sur une approche par niveaux de risque. Ce cadre, qui s'impose progressivement comme une norme internationale, doit inspirer le développement d'un cadre national adapté au contexte local.

5.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS5.1	Développer un cadre national d'IA éthique et responsable	2027
OS5.2	Créer un environnement réglementaire propice à l'innovation numérique	2026-2030
OS5.3	Positionner l'ARDIN comme acteur de référence sur la gouvernance de l'IA	2028
OS5.4	Développer les usages de l'IA au sein de l'ARDIN	2026-2028
OS5.5	Contribuer à l'émergence d'une industrie numérique nationale compétitive	2026-2030

5.3 Programmes Prioritaires

Programme 5.A — AI Governance Framework Élaboration d'un cadre national de gouvernance de l'IA, incluant une cartographie des usages à risque, un référentiel d'audit des systèmes d'IA, et des lignes directrices éthiques.

Programme 5.B — Regulatory Sandbox Mise en place d'un "bac à sable réglementaire" permettant aux startups et innovateurs de tester leurs solutions numériques dans un cadre sécurisé et supervisé.

Programme 5.C — ARDIN Digital Innovation Modernisation des outils internes de l'ARDIN par l'intégration de solutions d'IA pour améliorer l'efficacité opérationnelle (traitement des plaintes, veille réglementaire, analyse des données).

Programme 5.D — Observatoire de l'IA Création d'un observatoire national des usages et des impacts de l'IA, en partenariat avec les universités et centres de recherche.

5.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A5.1	Création du groupe de travail IA éthique (multistakeholder)	Dir. Générale	T1 2026
A5.2	Publication des lignes directrices nationales sur l'IA	Dir. Juridique	T3 2026
A5.3	Déploiement d'outils IA internes (analyse des plaintes)	Dir. Technique	T4 2026
A5.4	Lancement du Regulatory Sandbox	Dir. Générale	T2 2027
A5.5	Publication du Rapport national sur l'IA et les droits	Dir. Juridique	T3 2027
A5.6	Création de l'Observatoire National de l'IA	Dir. Coopération	T1 2028
A5.7	Organisation de la 1ère Conférence Nationale IA & Gouvernance	Dir. Générale	T2 2028
A5.8	Publication du référentiel d'audit des systèmes d'IA	Dir. Juridique	T3 2028
A5.9	Bilan du Regulatory Sandbox (première cohorte)	Dir. Générale	T4 2028
A5.10	Rapport d'impact de l'IA sur l'économie nationale	Dir. Coopération	T2 2030

5.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Cadre national IA adopté	Non	Oui	Révisé
Nombre de startups accompagnées via le Sandbox	0	15	50
% de traitements ARDIN assistés par IA	0 %	30 %	60 %
Nombre de publications sur la gouvernance de l'IA	0	5	15
Nombre de plaintes liées à l'IA traitées	-	30	150

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Nombre de partenariats académiques IA	2	6	12
Délai de traitement des dossiers (gain IA)	-	-20 %	-40 %

AXE STRATÉGIQUE 6 : COOPÉRATION NATIONALE ET INTERNATIONALE

6.1 Contexte

La gouvernance de l'Internet est par nature un sujet transnational qui ne peut être abordé efficacement par un acteur national isolé. L'ARDIN doit développer et entretenir un réseau dense de partenariats stratégiques, aussi bien au niveau national (avec les ministères, les régulateurs sectoriels, le secteur privé et la société civile) qu'international (avec les organisations multilatérales, les régulateurs homologues et les réseaux thématiques).

6.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS6.1	Conclure 5 nouvelles conventions de coopération internationale	2028
OS6.2	Renforcer la coordination avec les régulateurs nationaux	2026-2027
OS6.3	Développer des partenariats de coopération Sud-Sud	2027-2030
OS6.4	Contribuer activement aux normes internationales en matière numérique	2026-2030
OS6.5	Mobiliser des ressources financières internationales (5 M€)	2026-2030

6.3 Programmes Prioritaires

Programme 6.A — Diplomatie Numérique Renforcement de la présence de l'ARDIN dans les enceintes internationales (ICANN, IGF, UIT, Conseil de l'Europe, Union Africaine numérique), développement de positions nationales concertées sur les grandes questions de gouvernance Internet.

Programme 6.B — Réseau des Régulateurs Développement de conventions de coopération bilatérales et multilatérales avec les autorités de protection des données et de régulation numérique des pays partenaires.

Programme 6.C — Coopération Technique Sud-Sud Programme de partage d'expérience et de renforcement des capacités avec les organisations sœurs des pays en développement, notamment dans les domaines du DNS, de la cybersécurité et de la protection des données.

Programme 6.D — Mobilisation des Ressources Développement d'une stratégie de mobilisation des ressources externes (fonds UE, UIT, Banque Mondiale, programmes de coopération bilatérale) pour cofinancer les projets prioritaires de l'ARDIN.

6.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A6.1	Cartographie des partenaires stratégiques prioritaires	Dir. Coopération	T1 2026
A6.2	Signature de 2 accords de coopération (régulateurs régionaux)	Dir. Générale	T3 2026
A6.3	Adhésion au réseau FIRST (CERTs internationaux)	Dir. Cybersécurité	T4 2026
A6.4	Signature de la convention cadre avec l'UIT	Dir. Générale	T1 2027
A6.5	Organisation d'un atelier de coopération Sud-Sud	Dir. Coopération	T3 2027
A6.6	Soumission de 3 projets aux fonds européens	Dir. Coopération	T1-T3 2027
A6.7	Accueil d'une délégation de régulateurs partenaires	Dir. Générale	T2 2028
A6.8	Publication d'un rapport annuel de coopération internationale	Dir. Coopération	2026-2030 (annuel)

Code	Action	Responsable	Échéance
A6.9	Participation au Sommet de l'IA (représentation officielle)	Dir. Générale	T4 2028
A6.10	Bilan quinquennal des partenariats internationaux	Dir. Coopération	T3 2030

6.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Nombre de conventions de coopération actives	3	8	15
Ressources externes mobilisées (k€ cumulé)	200	1 500	5 000
Nombre d'événements internationaux avec présence ARDIN	4	10	18
Nombre de pays dans le réseau de coopération Sud-Sud	2	6	12
Nombre de contributions aux normes internationales	1	5	12
Nombre de missions d'assistance technique fournies	0	3	8

AXE STRATÉGIQUE 7 : RENFORCEMENT INSTITUTIONNEL DE L'ARDIN

7.1 Contexte

Pour accomplir les ambitions définies dans ce plan stratégique, l'ARDIN doit impérativement renforcer ses propres capacités institutionnelles. Cela implique d'investir dans ses ressources humaines, ses systèmes d'information, sa gouvernance interne, sa visibilité et sa crédibilité. Un régulateur fort, bien doté et reconnu est la condition sine qua non de l'efficacité réglementaire.

7.2 Objectifs Stratégiques

Code	Objectif Stratégique	Horizon
OS7.1	Renforcer les effectifs et les compétences des équipes ARDIN	2026-2028
OS7.2	Moderniser les systèmes d'information et l'infrastructure IT	2026-2027
OS7.3	Améliorer la gouvernance et la transparence institutionnelle	2026-2030
OS7.4	Accroître la notoriété et la visibilité de l'ARDIN	2026-2030
OS7.5	Assurer la pérennité financière de l'institution	2026-2030

7.3 Programmes Prioritaires

Programme 7.A — Capital Humain Plan de recrutement et de développement des compétences, mise en place d'une politique RH structurée, programme de formation continue pour l'ensemble du personnel.

Programme 7.B — Modernisation IT Refonte du système d'information interne, déploiement d'outils de gestion documentaire et de collaboration, sécurisation de l'infrastructure IT de l'ARDIN.

Programme 7.C — Gouvernance & Redevabilité Révision des textes organiques, renforcement du contrôle interne, publication de rapports d'activité annuels détaillés, mise en place d'un système de gestion de la performance organisationnelle.

Programme 7.D — Communication & Influence Développement d'une stratégie de communication institutionnelle, refonte du site web, présence renforcée sur les réseaux sociaux, organisation d'événements thématiques.

7.4 Actions à Mettre en Œuvre

Code	Action	Responsable	Échéance
A7.1	Réalisation d'un audit organisationnel complet	Dir. Générale	T1 2026

Code	Action	Responsable	Échéance
A7.2	Recrutement de 15 profils spécialisés	Dir. Générale / RH	T2-T4 2026
A7.3	Déploiement du nouveau système d'information	Dir. Technique	T3 2026
A7.4	Refonte du site web de l'ARDIN	Dir. Communication	T4 2026
A7.5	Publication du premier Rapport Annuel public	Dir. Générale	T1 2027
A7.6	Mise en place du Tableau de Bord Stratégique	Dir. Générale	T2 2027
A7.7	Lancement de la revue "ARDIN Numérique" (publication semestrielle)	Dir. Communication	T3 2027
A7.8	Révision des textes organiques de l'ARDIN	Dir. Juridique	T4 2027
A7.9	Certification ISO 9001 de l'ARDIN	Dir. Générale	T2 2028
A7.10	Évaluation institutionnelle externe	Dir. Générale	T4 2028
A7.11	Révision à mi-parcours du Plan Stratégique	Dir. Générale	T2 2028

7.5 Résultats Attendus et KPIs

Indicateur de Performance (KPI)	Baseline 2025	Cible 2027	Cible 2030
Effectif total de l'ARDIN	28	50	75
% du personnel avec formation continue/an	30 %	70 %	90 %
Indice de satisfaction du personnel	-	72/100	80/100
Disponibilité des systèmes IT (SLA interne)	95 %	99 %	99,9 %
Notoriété institutionnelle (enquête nationale)	18 %	35 %	55 %
Délai de publication du Rapport Annuel	> 6 mois	3 mois	2 mois
Taux d'exécution budgétaire annuel	72 %	85 %	92 %
Diversité de genre dans les équipes	31 % F	45 % F	50 % F

PARTIE VI — FEUILLE DE ROUTE QUINQUENNALE

6.1 Vision d'Ensemble par Année

Année 2026 — « Fondations »

Thème : Mise en place des bases, lancement des chantiers structurants

Les priorités de 2026 sont la structuration interne, le démarrage des chantiers réglementaires fondamentaux, le lancement du CERT-ARDIN, la modernisation de l'infrastructure DNS/DNSSEC et le déploiement des premiers outils numériques citoyens.

Jalons critiques 2026 :

- Création du CERT-ARDIN
- Déploiement DNSSEC à 100 %
- Lancement de la plateforme de dépôt de plaintes en ligne

- Publication du Référentiel National de Compétences Numériques
- Recrutement de 15 nouveaux profils spécialisés

Année 2027 — « Accélération »

Thème : Montée en puissance des programmes et consolidation des partenariats

2027 voit le déploiement généralisé des programmes lancés en 2026, l'intensification des partenariats nationaux et internationaux, le lancement du label "Confiance Numérique" et du Regulatory Sandbox, et la première évaluation intermédiaire des KPIs.

Jalons critiques 2027 :

- Formation de 200 DPO publics et privés
- Lancement du Regulatory Sandbox IA
- Premier Forum National de Gouvernance de l'Internet (FNGI)
- Signature de la convention avec l'UIT
- 65 % d'administrations publiques conformes RGPD

Année 2028 — « Consolidation »

Thème : Évaluation à mi-parcours et ajustements stratégiques

2028 est l'année de la maturité opérationnelle des programmes, avec l'évaluation à mi-parcours du Plan Stratégique (T2 2028), les ajustements nécessaires, l'obtention de la certification ISO 9001 et l'atteinte de plusieurs cibles intermédiaires majeures.

Jalons critiques 2028 :

- Évaluation à mi-parcours du Plan Stratégique
- 100 % des administrations publiques conformes (protection des données)
- Publication du référentiel national de certification cybersécurité
- Création de l'Observatoire National de l'IA
- 15 centres numériques de proximité opérationnels

Année 2029 — « Optimisation »

Thème : Ajustements fins et préparation de la phase finale

2029 est consacrée à l'optimisation des programmes en cours, au lancement de nouvelles initiatives issues des enseignements à mi-parcours, et à la préparation des bilans finaux.

Jalons critiques 2029 :

- 60 % de déploiement IPv6 atteint
- 40 000 citoyens formés au numérique (cumulé)
- Extension à 30 centres numériques de proximité
- Création de l'observatoire national des cybermenaces

Année 2030 — « Rayonnement »

Thème : Bilan, consolidation et projection vers 2035

2030 est l'année du bilan et de la démonstration des résultats. L'ARDIN publie son rapport quinquennal d'impact, lance la réflexion sur le Plan Stratégique 2031-2035, et consolide son positionnement comme institution de référence de la gouvernance numérique nationale.

Jalons critiques 2030 :

- 50 000 citoyens formés (cible atteinte)
- 85 % de taux de pénétration Internet national
- -40 % d'incidents cybersécurité majeurs
- 200 000 noms de domaine ccTLD enregistrés
- Publication du Rapport d'Impact Quinquennal ARDIN

6.2 Tableau de Bord Synoptique de la Feuille de Route

Programme / Action Clé	2026	2027	2028	2029	2030
CERT-ARDIN	Création	Opérationnel	Consolidation	Extension	Maturité
DNSSEC ccTLD	100 %	Maintien	Maintien	Maintien	Maintien
Transition IPv6	Plan lancé	35 %	50 %	60 %	60 %+
Protection données (conformité admin)	23 % → 30 %	65 %	100 %	Maintien	Maintien
Formation DPO	50 formés	300	500	650	800
Centres numériques proximité	5	15	20	25	30
Citoyens formés (cumulé)	3 000	15 000	28 000	40 000	50 000
Regulatory Sandbox IA	Préparation	Lancement	30 startups	40 startups	50 startups
Coopérations internationales	5	8	11	13	15
Effectif ARDIN	43	55	65	70	75

PARTIE VII — BUDGET PRÉVISIONNEL INDICATIF

7.1 Budget Global par Axe Stratégique (en milliers d'euros)

Axe Stratégique	2026	2027	2028	2029	2030	TOTAL
Axe 1 — Gouvernance Internet	750	700	600	600	550	**3 200**
Axe 2 — Protection des données	650	600	550	500	500	**2 800**
Axe 3 — Cybersécurité	1 200	1 000	800	800	700	**4 500**
Axe 4 — Compétences numériques	400	550	550	500	400	**2 400**
Axe 5 — Innovation & IA	500	700	700	600	600	**3 100**

Axe Stratégique	2026	2027	2028	2029	2030	TOTAL
Axe 6 — Coopération	300	400	400	350	350	**1 800**
Axe 7 — Renforcement institutionnel	550	500	450	400	300	**2 200**
TOTAL ANNUEL	**4 350**	**4 450**	**4 050**	**3 750**	**3 400**	**20 000**

7.2 Répartition par Nature de Dépense

Nature de Dépense	% du Budget Total	Montant total (k€)
Ressources humaines (recrutements, formations)	32 %	6 400
Infrastructure technique (DNS, cybersécurité, SI)	25 %	5 000
Programmes de sensibilisation et formation	18 %	3 600
Études, recherches et publications	8 %	1 600
Coopération et représentation internationale	7 %	1 400
Fonctionnement et frais généraux	6 %	1 200
Réserve stratégique et imprévus	4 %	800
TOTAL	**100 %**	**20 000**

7.3 Sources de Financement Prévisionnelles

Source de Financement	Montant indicatif (k€)	% du total
Budget public national (subvention d'État)	10 000	50 %
Redevances d'enregistrement ccTLD	3 500	17,5 %
Fonds européens et programmes multilatéraux	3 000	15 %
Coopération bilatérale et aide au développement	2 000	10 %
Recettes propres (certifications, formations)	1 500	7,5 %
TOTAL	**20 000**	**100 %**

7.4 Analyse Coût-Bénéfice Indicative

L'investissement de 20 000 k€ sur la période 2026-2030 génère des retombées économiques et sociales significatives, estimées selon les méthodes de valorisation des externalités positives utilisées par l'OCDE et la Banque Mondiale :

Domaine de bénéfice	Valeur économique estimée (k€)	Méthode
Réduction des coûts des cyberattaques (-40 %)	12 000	Coût évité
Croissance économie numérique (contribution ARDIN)	25 000	PIB additionnel
Gains d'efficacité administration (conformité données)	8 000	Productivité
Inclusion numérique (50 000 formés)	6 000	Insertion pro.
Confiance numérique (label, certification)	4 000	Valeur de marché
Total bénéfices estimés	**55 000**	
Ratio coût/bénéfice	**1 : 2,75**	

PARTIE VIII — MÉCANISMES DE SUIVI ET D'ÉVALUATION

8.1 Architecture du Système de Suivi-Évaluation

Le Plan Stratégique 2026-2030 sera doté d'un système de suivi et d'évaluation rigoureux, articulé à trois niveaux :

Niveau 1 — Suivi Opérationnel (mensuel/trimestriel)

- Revue mensuelle des actions en cours par les directeurs opérationnels ;
- Rapport trimestriel de suivi des KPIs transmis au Directeur Général ;
- Mise à jour du tableau de bord stratégique.

Niveau 2 — Évaluation Annuelle (semestrielle/annuelle)

- Rapport semestriel d'avancement transmis au Conseil d'Administration ;
- Rapport annuel public d'activité et de performance ;
- Évaluation des risques et ajustements des priorités.

Niveau 3 — Évaluation Stratégique (2028 et 2030)

- Évaluation à mi-parcours en 2028, par une équipe indépendante externe ;
- Évaluation finale en 2030, avec rapport d'impact quinquennal.

8.2 Indicateurs Globaux de Succès du Plan Stratégique

Indicateur Global	Baseline 2025	Cible 2028	Cible 2030
Taux de pénétration Internet	62 %	75 %	85 %
Indice national de cybersécurité (GCI-UIT)	45/100	65/100	78/100
% population avec compétences numériques de base	41 %	58 %	70 %
Conformité protection données (administrations)	23 %	100 %	100 %
Nombre d'incidents cyber majeurs	124/an	80/an	75/an
Indice de confiance numérique (enquête citoyens)	32 %	50 %	65 %
Notoriété de l'ARDIN	18 %	40 %	55 %
Taux d'exécution du Plan Stratégique	-	≥ 80 %	≥ 90 %

8.3 Tableau de Bord Stratégique (Dashboard)

L'ARDIN déploiera, dès le premier semestre 2027, un tableau de bord stratégique numérique accessible en ligne, présentant en temps réel l'état d'avancement du Plan Stratégique pour les indicateurs clés. Ce dashboard comprendra :

- **Indicateurs de niveau stratégique** : avancement global du plan, taux d'exécution budgétaire, évolution des KPIs par axe ;
- **Indicateurs de niveau opérationnel** : état d'avancement des actions, jalons atteints, alertes sur les retards ;
- **Infographies thématiques** : état de la cybersécurité nationale, évolution du ccTLD, cartographie des partenaires ;
- **Rapports téléchargeables** : rapports trimestriels, annuels et évaluations externes.

8.4 Processus de Reporting

Type de Rapport	Fréquence	Destinataires	Publication
Note de suivi opérationnel	Mensuelle	Directeurs	Interne
Rapport de KPIs trimestriel	Trimestrielle	DG + CA	Interne
Rapport semestriel d'avancement	Semestrielle	CA	Interne
Rapport Annuel d'Activité et Performance	Annuelle	CA + Public	Publique
Évaluation à mi-parcours	2028	CA + Tutelle + Public	Publique
Rapport d'Impact Quinquennal	2030	Toutes parties prenantes	Publique

---

PARTIE IX — GOUVERNANCE DU PLAN STRATÉGIQUE

9.1 Instances de Pilotage

Le Comité de Pilotage Stratégique (CPS)

Présidé par le Directeur Général, le CPS est l'instance de gouvernance centrale du Plan Stratégique. Il se réunit mensuellement pour examiner l'avancement des axes stratégiques, valider les ajustements opérationnels et arbitrer les priorités en cas de contraintes. Il est composé du DG, des directeurs de département, du responsable de la planification stratégique et d'un représentant du Conseil d'Administration.

Le Comité de Suivi du Conseil d'Administration (CSCA)

Le Conseil d'Administration désigne en son sein un Comité de Suivi dédié au Plan Stratégique, composé de 5 membres (dont au moins un expert technique indépendant et un représentant de la société civile). Ce comité reçoit les rapports trimestriels et formule des recommandations stratégiques à l'intention du CA plénier.

Les Référents Stratégiques par Axe

Chaque axe stratégique est placé sous la responsabilité d'un Référent Stratégique, désigné parmi les cadres supérieurs de l'ARDIN. Les Référents Stratégiques sont garants de la mise en œuvre de leur axe et rendent compte mensuellement au CPS.

La Commission Multipartite de Suivi

Pour assurer la redevabilité vis-à-vis des parties prenantes externes, une Commission Multipartite de Suivi (CMS) est créée, composée de représentants des ministères partenaires, du secteur privé, de la société civile et du monde académique. Elle se réunit semestriellement et émet un avis public sur l'avancement du Plan Stratégique.

9.2 Principes de Gouvernance du Plan

Principe	Application concrète
Redevabilité	Publication obligatoire des rapports annuels et des évaluations
Participation	Consultation multipartite lors des révisions du plan
Agilité	Possibilité d'ajustements annuels des programmes et budgets
Transparence	Tableau de bord public accessible en ligne
Intégration	Alignement du plan sur les priorités nationales et les ODD

PARTIE X — GESTION DES RISQUES

10.1 Matrice des Risques Stratégiques

Code	Risque	Probabilité	Impact	Niveau de Risque
R01	Insuffisance de financement public	Moyenne	Élevé	**Élevé**
R02	Pénurie de compétences spécialisées	Haute	Élevé	**Critique**
R03	Cyberattaque majeure contre les infrastructures de l'ARDIN	Moyenne	Critique	**Critique**
R04	Changements réglementaires imprévisibles	Moyenne	Moyen	**Moyen**
R05	Résistance au changement en interne	Faible	Moyen	**Faible**
R06	Non-adhésion des parties prenantes aux programmes	Moyenne	Élevé	**Élevé**
R07	Évolution technologique dépassant le cadre prévu	Haute	Élevé	**Critique**
R08	Instabilité géopolitique et fragmentation d'Internet	Faible	Critique	**Élevé**
R09	Insuffisance des capacités de suivi-évaluation	Moyenne	Moyen	**Moyen**
R10	Turnover élevé du personnel clé	Moyenne	Élevé	**Élevé**

10.2 Stratégies de Mitigation des Risques Critiques

Risque R02 — Pénurie de compétences

Stratégie : Développer une politique RH attractive (rémunération compétitive, formation continue, plan de carrière), créer des partenariats avec les universités, développer le télétravail pour attirer des talents hors de la capitale.

Risque R03 — Cyberattaque contre l'ARDIN

Stratégie : Audit de sécurité de l'infrastructure IT de l'ARDIN dès 2026, déploiement d'un SOC dédié, plan de continuité d'activité et de reprise après sinistre, formation spécialisée des équipes IT.

Risque R07 — Évolution technologique

Stratégie : Mise en place d'une cellule de veille technologique permanente, participation aux forums internationaux de prospective numérique, intégration d'une clause de révision annuelle dans le Plan Stratégique.

10.3 Plan de Contingence

En cas de matérialisation d'un risque critique (R02, R03, R07), l'ARDIN activera un Plan de Contingence prédéfini comprenant :

1. **Déclencheur** : Identification formelle du risque matérialisé par le CPS ;
2. **Évaluation d'impact** : Analyse rapide des conséquences sur les axes stratégiques concernés ;
3. **Ajustements** : Réallocation des ressources, report ou accélération de certains programmes ;
4. **Communication** : Information transparente du Conseil d'Administration et des parties prenantes ;
5. **Révision** : Mise à jour du plan de gestion des risques.

CONCLUSION

Le Plan Stratégique 2026-2030 de l'Association Nationale de Régulation des Domaines et de l'Internet représente bien plus qu'un document de planification institutionnelle : il est le reflet d'un engagement collectif, solennel et mesurable envers les citoyens, les entreprises et les institutions de notre pays.

En adoptant ce plan, l'ARDIN affirme sa volonté de se hisser au niveau des meilleures pratiques internationales en matière de gouvernance numérique, tout en restant profondément ancrée dans les réalités et les besoins de sa société. Les sept axes stratégiques définis dans ce document constituent un programme ambitieux mais réaliste, qui tient compte à la fois des ressources disponibles et des défis exceptionnels que pose la révolution numérique à nos institutions et à nos citoyens.

L'ambition de l'ARDIN pour 2030 est claire : faire du numérique national un espace de confiance, d'opportunité et de protection pour chacun. Cela suppose une gouvernance Internet robuste et représentative, une protection effective des données personnelles, un niveau de cybersécurité à la hauteur des menaces contemporaines, des compétences numériques largement diffusées dans la population, un cadre éthique pour l'innovation et l'intelligence artificielle, des partenariats internationaux solides, et une institution ARDIN forte, reconnue et pérenne.

Ces résultats ne s'obtiendront pas seuls. Ils requièrent l'engagement des pouvoirs publics, la mobilisation du secteur privé, la participation active de la société civile, et le soutien de la communauté internationale. L'ARDIN se positionne résolument comme le catalyseur de cette mobilisation collective.

Le chemin est tracé. La volonté est réelle. La confiance numérique de demain se construit aujourd'hui.

« L'Internet n'est pas une finalité en soi. Il est un instrument au service du développement humain, de la démocratie et de la dignité. Notre rôle est de veiller à ce qu'il reste ce qu'il a toujours promis d'être : une infrastructure ouverte, libre et au service de tous. »

— Direction Générale de l'ARDIN

ANNEXES

Annexe A — Glossaire

Terme	Définition
ccTLD	Country Code Top-Level Domain — Extension de domaine de premier niveau rattachée à un pays (ex : .fr, .sn, .ma)
CERT	Computer Emergency Response Team — Équipe de réponse aux incidents de cybersécurité
DPO	Data Protection Officer — Délégué à la Protection des Données
DNS	Domain Name System — Système de noms de domaine, l'annuaire de l'Internet
DNSSEC	DNS Security Extensions — Extension sécurisée du DNS
GCI	Global Cybersecurity Index — Indice mondial de cybersécurité de l'UIT
ICANN	Internet Corporation for Assigned Names and Numbers — Organisation gérant les ressources d'adressage Internet
IGF	Internet Governance Forum — Forum sur la Gouvernance de l'Internet (ONU)
IPv6	Internet Protocol version 6 — Nouvelle version du protocole d'adressage Internet
KPI	Key Performance Indicator — Indicateur clé de performance
RGPD	Règlement Général sur la Protection des Données (UE)
SOC	Security Operations Center — Centre opérationnel de sécurité
UIT	Union Internationale des Télécommunications

Annexe B — Cadres de Référence Internationaux

Organisation	Document de référence	Pertinence pour l'ARDIN
ICANN	Politiques du ccNSO et du GNSO	Gouvernance des noms de domaine
UIT	Global Cybersecurity Agenda	Stratégie nationale de cybersécurité
UE	RGPD, AI Act, NIS2, eIDAS	Protection données, IA, cybersécurité
ONU/IGF	Rapport du Groupe de Haut Niveau Digital Compact	Gouvernance globale de l'Internet
UNESCO	Recommandation sur l'IA éthique (2021)	Éthique de l'IA
OCDE	Principes sur l'IA (2019)	Politique nationale IA
Banque Mondiale	Digital Development Partnership	Inclusion numérique

Annexe C — Liste des Abréviations

ARDIN, CERT, ccTLD, DNS, DNSSEC, DPO, GCI, ICANN, IGF, IPv6, KPI, NIS2, OCDE, ODD, ONU, PME, RGPD, SOC, UIT, UNESCO

— FIN DU DOCUMENT —

Plan Stratégique 2026-2030 de l'ARDIN Document officiel approuvé par le Conseil d'Administration Référence : ARDIN/PS/2026-2030/V1.0 — Juin 2026 Tous droits réservés — ARDIN

Ce document a été élaboré selon un processus consultatif multipartite, en conformité avec les meilleures pratiques des organisations internationales spécialisées dans la gouvernance de l'Internet et du numérique.