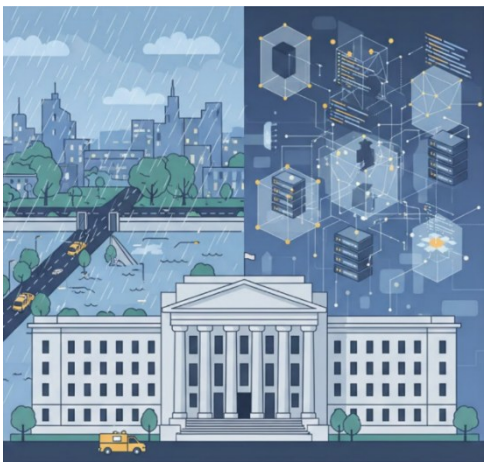
Gestion des crises et état d’exception

Pandémies, catastrophes, cyberattaques. Cadres juridiques.



Les États qui gouvernent bien en temps de crise ne le doivent généralement pas à la chance ou au génie de leurs dirigeants. Ils le doivent à des décisions prises bien avant la crise, par des législateurs qui avaient pris la peine d'imaginer le pire et de le traduire en droit. Les pandémies, les catastrophes naturelles et les cyberattaques ne surgissent pas par surprise dans un monde bien informé: ce sont des risques structurels identifiables, documentés par les agences de sécurité sanitaire, les services météorologiques et les centres d'analyse de la menace informatique. La question pertinente est donc de décider selon quels cadres juridiques ces trois familles de crises seront gérées le jour où elles se produisent, plutôt que de se demander si elles surviendront.

L'état d'exception, tel que le comprend le droit constitutionnel comparé, désigne un régime juridique particulier qui autorise l'exercice temporaire de pouvoirs élargis sans suspendre le droit lui-même. Cette distinction sépare les démocraties qui ont réfléchi la crise en amont de celles qui s'y abandonnent. Carl Schmitt soutenait, dans Théologie politique (1922), que "est souverain celui qui décide de l'état d'exception", faisant de cette capacité de décision le coeur même du politique. Giorgio Agamben, dans State of Exception (2005), retournait l'argument: lorsque les pouvoirs d'urgence s'installent dans la durée, la démocratie se vide progressivement de son contenu sans que personne n'ait formellement décidé de la supprimer. Ces deux lectures définissent une exigence pratique: les pouvoirs exceptionnels doivent exister et rester suffisamment forts pour être efficaces, tout en demeurant bornés dans le temps et contrôlés dans leur exercice. Cette double exigence se résout par le droit positif, à travers quatre principes vérifiables.

Les pouvoirs exceptionnels doivent être prévus par la loi avant la crise, de sorte qu'aucun gouvernement ne les invente dans l'urgence selon ses intérêts du moment. Leur déclenchement doit reposer sur des critères objectifs définis à froid: seuils épidémiques mesurables, ampleur territoriale précise d'une catastrophe, niveau quantifié de dommage d'une attaque informatique. On peut objecter que ces critères restent fixés par le pouvoir politique lui-même, qui pourrait théoriquement les calibrer à son avantage. C'est exact, mais cela ne fragilise pas le principe: l'enjeu n'est pas d'éliminer toute décision politique, ce qui est impossible, mais de la déplacer en amont de la crise, à un moment où aucun gouvernement ne sait encore s'il bénéficiera ou non des pouvoirs qu'il définit. Cette incertitude sur l'identité du futur bénéficiaire discipline le calibrage des seuils bien mieux qu'un contrôle a posteriori, puisque le législateur d'aujourd'hui ignore qui gouvernera lors de la prochaine crise. Leur prolongation doit requérir une validation parlementaire explicite, avec des délais fixes, pour éviter que l'exception ne se reconduise par inertie bureaucratique. Leur application doit demeurer justiciable devant les tribunaux, garantissant un recours réel aux personnes affectées. L'absence de ces garde-fous produit des trajectoires documentées. En Hongrie, le Parlement a adopté le 30 mars 2020 une loi accordant au gouvernement de Viktor Orbán le pouvoir de légiférer par décret dans tous les domaines, sans limite de temps ni contrôle parlementaire effectif. Le Conseil de l'Europe, le Parlement européen, l'OSCE et plusieurs organisations de défense des droits humains ont dénoncé ce texte, qui exclut par ailleurs toute élection ou référendum pendant son application. La loi illustre exactement ce que les quatre principes cherchent à empêcher: une exception sans critères objectifs de déclenchement, sans terme fixé et sans contrôle parlementaire réel.

Ces dérives ont une réponse technique précise: les clauses de caducité automatique. Ce sont des dispositions qui éteignent les pouvoirs d'exception à une date certaine, sans qu'il soit nécessaire de voter pour les supprimer. Le mécanisme oblige le gouvernement à revenir devant le Parlement pour renouveler ses pouvoirs, plutôt que de compter sur l'inertie législative pour les conserver. Son absence aux États-Unis a produit un résultat révélateur: le USA PATRIOT Act, adopté en quarante-cinq jours après les attentats de 2001, a survécu plus de quatorze ans dans sa forme initiale et a été appliqué à des enquêtes criminelles ordinaires sans lien avec le terrorisme, comme l'a révélé l'affaire Snowden en 2013. La Suisse a utilisé sa loi sur les épidémies de 2012, révisée en 2016, pour encadrer sa réponse au Covid-19 avec une base légale préexistante et une révision parlementaire à mi-parcours. La France a adopté en mars 2020 une loi d'urgence sanitaire distincte des pouvoirs de crise de l'article 16 de la Constitution, précisément pour ne pas concentrer les décisions entre les mains du seul exécutif. On objecte parfois que la France a prolongé son état d'urgence sanitaire à six reprises entre 2020 et 2022, ce qui affaiblirait l'exemple. L'objection se retourne en réalité contre elle-même: chaque prolongation est passée par un débat et un vote au Parlement, avec des modifications du texte, un examen par le Conseil constitutionnel et une date de fin précise renégociée à chaque fois. Le système a fonctionné exactement comme prévu, en forçant le gouvernement à justifier publiquement la poursuite de ses pouvoirs plutôt qu'à les conserver par défaut. Ces choix démontrent qu'une doctrine de l'urgence rigoureuse peut s'élaborer à froid, avant que la crise n'éclate, et continuer à fonctionner sous la pression d'une crise qui dure.

La pandémie de Covid-19 a confirmé ce que les spécialistes de l'administration publique savaient depuis longtemps: l'improvisation institutionnelle coûte cher, en vies humaines, en dépenses publiques et en capital de confiance. On objecte parfois que les régimes autoritaires auraient mieux géré la crise sanitaire, en citant la Chine et ses confinements draconiens. L'argument résiste mal à l'examen. La Chine a dissimulé l'épidémie pendant plusieurs semaines décisives, faisant reposer sa gestion sur la coercition plutôt que sur l'adhésion volontaire. Les études comparatives publiées dans The Lancet et dans le Journal of Public Health entre 2021 et 2023 montrent que les pays à haute confiance institutionnelle ont obtenu des résultats épidémiques comparables ou supérieurs sans recourir à des restrictions aussi brutales. La Nouvelle-Zélande, la Corée du Sud et les pays scandinaves avaient investi avant 2020 dans des protocoles de communication de crise, des stocks stratégiques et des lignes de commandement précises. La confiance sociale que leurs populations ont manifestée tient à une transparence décisionnelle et à une prévisibilité du droit qui s'observent et se mesurent, bien davantage qu'à un quelconque attachement affectif envers leurs gouvernements.

Les cyberattaques posent un défi d'une nature particulière, parce qu'elles brouillent les frontières classiques entre sécurité intérieure, défense nationale et protection des infrastructures civiles. L'attaque NotPetya de 2017, officiellement attribuée à la Russie par les gouvernements américain, britannique et australien, a paralysé des hôpitaux ukrainiens, des banques, des terminaux portuaires et des entreprises comme Maersk et Merck dans plusieurs pays, causant plus de dix milliards de dollars de dommages mondiaux sans qu'aucune bombe n'ait été larguée. L'OTAN a reconnu formellement le cyberespace comme cinquième domaine opérationnel en 2016, confirmant que des attaques informatiques peuvent atteindre un seuil suffisant pour déclencher l'article 5 du Traité de Washington. Un État qui n'intègre pas la cybersécurité dans son droit public s'expose à deux risques symétriques: laisser des acteurs privés gérer des questions de souveraineté, ou dépendre d'alliés étrangers pour défendre ses propres infrastructures critiques. Des entreprises comme Microsoft, Cloudflare ou CrowdStrike protègent aujourd'hui des gouvernements entiers contre des attaques informatiques d'État. Cette dépendance est efficace à court terme et risquée à moyen terme, car elle transfère à des entités privées régies par le droit commercial américain des décisions touchant à l'intégrité des systèmes publics d'un pays souverain. Un cadre juridique de cybersécurité doit distinguer ce qui peut être externalisé, notamment la détection et la réponse technique, de ce qui doit rester sous contrôle public: la doctrine d'attribution des attaques, les seuils de riposte et la coordination avec les alliés.

Le risque croissant de crises composées ajoute une couche de complexité supplémentaire. Une cyberattaque ciblant les systèmes d'information hospitaliers pendant une pandémie, ou une catastrophe naturelle détruisant les infrastructures de communication au moment où un gouvernement doit coordonner une réponse sanitaire: ces scénarios illustrent comment les cadres juridiques conçus pour une seule catégorie de crise peuvent se révéler insuffisants face à des événements simultanés. Le ransomware qui a paralysé une partie du système de santé irlandais en mai 2021, en plein contexte pandémique, a montré qu'une infrastructure critique déjà sous tension sanitaire devient une cible d'autant plus attractive et d'autant plus vulnérable. Les crises composées exigent des protocoles interministériels préétablis et des lignes d'autorité claires entre les institutions chargées de la santé, de la défense et de la gestion du territoire. Des exercices réguliers, menés à froid, permettent de tester ces protocoles et d'identifier leurs lacunes avant qu'une crise réelle ne les révèle au pire moment possible.

La gestion des catastrophes naturelles illustre la même logique de souveraineté préparée. Elle se manifeste concrètement dans la capacité d'un État à mobiliser rapidement des ressources humaines et matérielles, à coordonner des acteurs dispersés sur le territoire et à maintenir l'égalité de traitement juridique entre les citoyens, y compris quand certaines régions sont coupées du reste du pays. L'égalité juridique en situation d'urgence exige que les ressources d'évacuation, les soins médicaux et les compensations financières soient distribuées selon des règles préétablies, et non selon la proximité politique ou géographique des décideurs avec les zones sinistrées. Les inondations au Pakistan en 2022 et les tremblements de terre en Turquie en 2023 ont montré comment l'absence de doctrine préétablie transforme une catastrophe naturelle en catastrophe institutionnelle, avec des délais de réponse mortels et une distribution inéquitable des secours. Hans Kelsen écrivait dans La démocratie (1920) que "la force de l'État de droit se mesure précisément à sa capacité de subsister dans l'exception." La robustesse d'un État se révèle sous pression maximale, rarement par temps calme.

Un État-Nation moderne qui prend sa propre pérennité au sérieux investit dans une doctrine de l'urgence avant d'en avoir besoin. Des textes de loi rédigés à froid, des critères de déclenchement objectifs, des clauses de caducité automatique, des protocoles interministériels testés régulièrement: ces instruments semblent bureaucratiques en période de stabilité. Ils deviennent vitaux quand la crise éclate. Les démocraties qui ont consacré cet effort légal et institutionnel ont traversé les grandes crises récentes avec moins de pertes et plus de légitimité que celles qui ont improvisé. Une exception bien encadrée renforce l'État de droit qu'elle est censée temporairement suspendre.

Louis-Martin Carrière