GOVERNANÇA E GESTÃO DE RISCOS DE DESASTRES TECNOLÓGICOS

Daniel Ardito
dbardito@gmail.com, Universidade Federal Fluminense

Resumo: Os desastres tecnológicos são males produzidos pelos seres humanos com consequências tão devastadoras quanto qualquer desastre natural que possa ter ameaçado ou ainda os ameace. A análise bibliográfica empreendida tem como objetivo apresentar uma proposta alternativa para o processo de gestão de riscos de desastres tecnológicos, alternativa essa que leve em consideração a participação dos potencialmente atingidos durante todo o processo, tanto por valorização dos aspectos objetivos, quanto subjetivos da percepção e do tratamento de riscos tecnológicos. O artigo foi desenvolvido mediante revisão bibliográfica e documental, visando correlacionar teorias de estudo sobre a governança e gestão de riscos e sobre desastres tecnológicos que, notadamente resultassem em proposta alternativa ao modelo atual de gestão de riscos de desastres tecnológicos. Os resultados da análise demonstram ser possível e viável um modelo de gestão de riscos de desastres tecnológicos que agregue, de forma justa, a participação dos potencialmente atingidos.

Palavras-chave: Desastres tecnológicos. Gestão de riscos. Governança.

Abstract: *Man-made disasters are evils produced by human beings with consequences as devastating as any natural disaster that may have threatened or still threatens human beings. The bibliographic analysis undertaken aims to present an alternative approach to the risk management process of man-made disasters, an alternative that takes into account the participation of those potentially affected throughout the process, both due to the positive appreciation of the objective and subjective aspects of perception and the treatment of technological risks. Through bibliographical and documentary review, aiming to correlate theories about governance and risk management and man-made disasters that, notably resulted in the proposal of an alternative to the current model of man-made disaster risk management. The results of the analysis demonstrate that a risk management model for man-made disasters that fairly aggregates the participation of those potentially affected is possible and viable.*

Keywords: *Man-made disaster. Risk management. Governance.*

Resumen: *Los desastres tecnológicos son males producidos por el ser humano con consecuencias tan devastadoras como cualquier desastre natural que los haya amenazado o amenazado. El análisis bibliográfico realizado tiene como objetivo presentar una propuesta alternativa para el proceso de gestión del riesgo de desastres tecnológicos, una alternativa que toma en cuenta la participación de los potencialmente afectados a lo largo del proceso, tanto valorando los aspectos objetivos como subjetivos de la percepción y el tratamiento de los riesgos tecnológicos. El artículo se desarrolló a través de una revisión bibliográfica y documental, con el objetivo de correlacionar las teorías de estudio sobre la gobernancia y gestión del riesgo y los desastres tecnológicos que, en particular, resultaron en la propuesta de una alternativa al modelo actual de gestión del riesgo tecnológico de desastres. Los resultados del análisis muestran que es posible y viable un modelo de gestión de riesgos de desastres tecnológicos que agregue de manera justa la participación de los potencialmente afectados.*

Palabras clave: Desastres tecnológicos. Gestión de riesgos. Gobernancia.

1. INTRODUÇÃO

Encaramos, mais do que nunca nos dias de hoje, infortúnios gerados por seres humanos, algumas vezes mais devastadores que qualquer outro desastre natural que porventura possa ter acometido nossos antepassados.

A reboque de todas as facilidades e modernidades que compõem o estilo de vida atual, temos uma infinidade de riscos que são autoproduzidos e contam com consequências que não respeitam demarcações legais ou fronteiras. Vivemos segundo Ulrich Beck (2010) em uma sociedade de riscos, onde um grande colapso pode se romper a qualquer instante, tragando vidas e destruindo o meio ambiente. Colapsos esses que podem ser gerados por riscos tecnológicos decorrentes, em sua maioria, da exploração econômica de organizações públicas ou privadas e que produzem vítimas que não tiveram qualquer chance de optar se o risco valia à pena ser corrido, ou se alguma vantagem decorrente desse risco compensasse a ele estar exposto.

Fazer gestão de riscos de desastres tecnológicos é um grande desafio. Para minimizar consequências e preservar vidas é fundamental procurar estruturas de gestão que busquem a convergência entre métodos objetivos e percepções subjetivas. Deve-se buscar um modelo participativo que entenda a importância que a preocupação das partes interessadas tem no processo.

A governança de risco proposta pelo *International risk governance council* (IRGC) se apresenta como alternativa possível para lidar de forma participativa com a gestão de riscos de desastres tecnológicos, fazendo com que esses fenômenos sejam tratados de forma justa e participativa, convertendo decisões privadas em decisões públicas, assim como são as consequências de uma eventual concretização do risco de desastres tecnológicos.

2. DESASTRES TECNOLÓGICOS

Na literatura nacional e internacional sobre desastres, assim como nos manuais técnicos dos órgãos de Defesa Civil espalhados pelo Brasil, há inúmeras definições do termo “desastre”.

Segundo o escritório das Nações Unidas para a Redução do Risco de Desastre (UNDRR), temos a seguinte definição:

> A serious disruption of the functioning of a community or a society at any scale due to hazardous events interacting with conditions of exposure, vulnerability and capacity, leading to one or more of the following: human, material, economic and environmental losses and impacts (UNDRR, 2019).

Adicionalmente à definição supracitada, consta ainda a seguinte anotação complementar:

> Annotations: The effect of the disaster can be immediate and localized, but is often widespread and could last for a long period of time. The effect may test or exceed the capacity of a community or society to cope using its own resources, and therefore may require assistance from external sources, which could include neighbouring jurisdictions, or those at the national or international levels. (UNDRR, 2019)

No Brasil, o extinto Ministério da Integração Nacional, ao qual a Secretaria Nacional de Proteção e Defesa Civil era subordinada, publicou em 2017 um glossário de Proteção e Defesa Civil. Nele, assim é definido desastre:

> Resultado de eventos adversos, naturais, tecnológicos ou de origem antrópica, sobre um cenário vulnerável exposto à ameaça, causando danos humanos, materiais ou ambientais e consequentes prejuízos econômicos e sociais. (BRASIL, 2017, p. 22)

Os desastres recorrentemente são diferenciados por sua origem. Portanto, na maior parte da literatura sobre o tema, encontraremos os termos desastres naturais, para se referir a desastres que tem sua origem em fenômenos da natureza, como terremotos, secas, deslizamentos de terra; desastres tecnológicos ou produzidos pela ação humana, relacionado aos desastres que tem sua origem associada à ação humana, como rompimento de barragens, acidentes em indústrias ou incêndios urbanos; e desastres mistos, quando um desastre natural pode desencadear um desastre tecnológico, como foi o caso do desastre envolvendo a usina nuclear de Fukushima no Japão, em 2011, onde um tsunami deu início ao colapso da usina.

No Brasil, até 2015 tínhamos a Codificação de Desastres, Ameaças e Riscos (CODAR), que adotava a divisão da origem dos desastres em três grandes grupos, podendo ser naturais, humanos ou mistos. No entanto, a partir de 2016, o CODAR foi substituído pela Classificação e Codificação Brasileira de Desastres (COBRADE), doravante documento oficial que regula a classificação de desastres no Brasil. Por ele os desastres passaram a ser enquadrados em dois grandes grupos. De acordo com sua origem, podem ser desastres naturais; ou tecnológicos.

Vale salientar, embora não seja o objetivo da nossa análise, que há alguma controvérsia acerca da assertividade da utilização do termo desastre natural, uma vez que parte das condições de ocorrência desse tipo de desastre está associada à forma como o ser humano ocupa e interage com o meio ambiente, assim como às vulnerabilidades que determinados territórios apresentam em decorrência da ausência do Estado. Por esta premissa, não há que se falar em desastre natural, mas sim, em alguns casos, desastre com uma das causas relacionadas a um evento natural.

Em relação à utilização da denominação desastres tecnológicos, desenvolvemos particularmente algumas ressalvas. Entendemos que o termo "tecnológico" induz muitas pessoas, intuitivamente, a imaginar que se trata de desastres envolvendo computadores ou altas tecnologias; e tenham certa dificuldade de associar o termo a um acidente envolvendo um navio ou ao rompimento de uma barragem, por exemplo. Ao nosso ver, o termo mais acertado a se utilizar seria desastres produzidos pela ação humana, como alguns países assim os categorizam e adotam em diversas práticas sociais. Em se tratando de percepção de riscos, quanto mais fácil e menos ambígua a comunicação, melhores podem ser os resultados de processos de conscientização de riscos.

Independente das colocações anteriores e das discussões suscitadas sobre a melhor forma de classificar a origem dos desastres, é unânime o entendimento que a classificação desses fenômenos é fundamental para a busca da compreensão e das medidas de prevenção e mitigação.

2.1 Desastres tecnológicos relevantes para o estudo da prevenção

São inúmeros os exemplos de desastres tecnológicos pelo mundo. No entanto, a seguir, escolhemos citar alguns deles porque marcaram, de alguma forma, a evolução do estudo prevencionista relacionado a esse fenômeno. Entre os casos a seguir apresentados, é possível identificar que as maiores vítimas são as populações involuntariamente expostas aos riscos.

Destacamos que cada desastre tem sua importância, não merecendo escala hierárquica, isto é, nenhum desastre é melhor ou pior que o outro. Afinal, para o afetado, recorrentemente o pior e mais significativo desastre será o que o atingiu. No entanto, considerar supostamente todos os desastres, inviabilizaria o presente estudo e demandaria milhares de páginas, além de se distanciar do foco do estudo. Ademais, a breve descrição a seguir de alguns desastres tecnológicos, não tem por objetivo ser fonte detalhada de estudos de cada um dos casos. Propomos tão somente criar uma trilha de reflexão sobre desastres tecnológicos construídos pelo homem e que impactaram diretamente populações que pouca relação guardava com a origem do risco.

- **Bophal – 1984:** Bophal é a capital do Estado de Madhya Pradesh, na região central da Índia. Também era endereço de uma fábrica da multinacional industrial americana *Union Carbine*, que produzia o pesticida carbaril.

Na madrugada de 03 de dezembro de 1984, Bophal entrou para a história dos desastres tecnológicos, quando um tanque, contendo 42 toneladas de isocianato de metila, foi inundado por água, gerando uma reação química que produziu uma nuvem de gazes venenosos lançada na atmosfera, contaminando e levando à morte milhares de pessoas.

> A nuvem tóxica afetou a cidade de Bhopal, com aproximadamente 800.000 habitantes. Ainda que as cifras de mortos e feridos sejam muito imprecisas, pode-se afirmar que essa emergência gerou entre 2.500 e 4.000 óbitos, além de 180.000 feridos. Muitos especialistas consideram esse evento o pior desastre ocorrido em toda história da indústria química. (Perez, 2016, p. 55)

O preparo das comunidades para enfrentar situações dessa natureza era inexistente em Bophal, assim como a capacidade de reação da própria *Union Carbine*, fatos esses que contribuíram para potencializar as consequências do desastre.

> A nuvem tóxica formada estendeu-se sobre áreas povoadas em direção ao sul, favorecidas por um vento leve e condições de inversões térmicas. Na área de Railway Colony, localizada a cerca de 2 km da unidade industrial, onde viviam aproximadamente 10.000 pessoas, verificou-se que, em 4 minutos, 150 pessoas morreram, 200 ficaram paralisadas, outras 600 inconscientes e por volta de 5.000 sofreram danos graves. Muitas tentaram fugir, mas seguiram a direção errada, contra a fase gasosa tóxica. (Perez, 2016, p. 57)

O desastre da *Union Carbine* em Bophal estabeleceu precedentes que nos ajudam a perceber como a lógica do lucro, muitas vezes a qualquer custo, bem como a ausência de uma gestão de riscos de desastres tecnológicos que considere as partes envolvidas (*stakeholders*) e, principalmente, as partes expostas a uma eventual consequência do risco assumido no âmbito privado, pode expor comunidades inteiras, culminando na morte de milhares de pessoas. Ele também corrobora a máxima interpretativa de Beck (2010) que atribui à pobreza extrema, um atrativo aos riscos extremos. Como visto, Bophal estava bem longe de ser uma cidade rica padrão dos Estados Unidos da América, país de origem da *Union Carbine*.

Três elementos principais compõem a sinistra equação que resultou nesse desastre. O primeiro relacionado à construção de uma indústria química de pesticidas, em área densamente povoada, sem tomar medidas para evitar que áreas vizinhas não fossem ocupadas, ou ainda criar um plano de segurança e conscientização para os moradores vizinhos quanto aos riscos existentes. O segundo relacionado à tecnologia obsoleta e aos padrões de segurança aquém dos praticados pelas coirmãs americanas. O terceiro corresponde a acentuados desinvestimentos orientados a melhorar os resultados financeiros da empresa e que, ao final, impactaram diretamente as medidas de segurança da fábrica (MARTINS, 2016).

- **Chernobyl – 1986:** Em 26 de abril de 1986, a humanidade testemunhou o que muitos temiam. Essa foi a data do pior desastre nuclear da história, a explosão do reator 4 da usina nuclear de Chernobyl na Ucrânia, até então, território da URSS (União das Repúblicas Socialistas Soviéticas). Chama atenção,

> entre outros fatores, que a usina de Chenobyl, assim como centenas outras, espalhadas pelo globo eram tidas, por seus especialistas, como ambientes extremamente seguros e com riscos desprezíveis para as comunidades que as cercavam.
>
> > Longe daqui, no oeste da União Soviética, ou seja, de agora em diante, em nosso entorno próximo, aconteceu um acidente - nada deliberado ou agressivo, na verdade algo que de fato deveria ser evitado, mas que, por seu caráter excepcional, também é normal, ou mais, é humano mesmo. Não é a falha que produz a catástrofe, mas os sistemas que transformam a humanidade do erro em inconcebíveis forças destrutivas. Para a avaliação dos perigos, todos dependem de instrumentos de medição, de teorias e, sobretudo: de seu desconhecimento - inclusive os especialistas que ainda há pouco haviam anunciado o império de 10 mil anos de segurança probabilística atômica e que agora enfatizam, com uma segurança renovada de tirar o fôlego, que o perigo jamais seria agudo. (BECK, 2011, p. 8)

Nesse desastre, mais que em qualquer outro até então ocorrido, é possível identificar duas das principais características que compõem a sociedade de risco: a autoprodução do risco e suas consequências globais, conceito esse cunhado por Beck (2010).

Em se tratando de autoprodução do risco, o caso de Chernobyl é óbvio e por si só explicativo. Trata-se de uma usina concebida para atender os anseios energéticos de uma nação, ou seja, a solução para a falta de energia traz consigo o risco de um acidente nuclear.

Svetlana Aleksiévitch, escritora vencedora do prêmio Nobel de literatura, em seu livro "Vozes de Tchernóbil" cita um trecho do trabalho da Escola Superior Internacional de Radiologia Sákharov de 1992 que evidencia o caráter global das consequências desse desastre:

> > De acordo com observações diversas, em 29 de abril de 1986 foram registrados altos níveis de radiação na Polônia, na Alemanha, na Áustria e na Romênia; em 30 de abril, na Suíça e no norte da Itália; nos dias 1º 2 de maio, na França, na Bélgica, nos Países Baixos, na Grã-Bretanha e no norte da Grécia; em 3 de maio, em Israel, no Kuwait e na Turquia...
> >
> > Projetadas a grandes alturas, as substâncias gasosas e voláteis se dispersaram pelo globo: em 2 de maio foram registradas no Japão, na China; no dia 5, na Índia; e em 5 e 6 de maio nos Estados Unidos e no Canadá.
> >
> > Em menos de uma semana, Tchernóbil se tornou um problema para o mundo inteiro. (ALEKSIÉVITCH, 2016, p. 11)

Os números oficiais do desastre de Chernobyl são muito questionáveis. Diversas fontes divergem sobre a quantidade de mortos diretos e indiretos, mas é inegável e

lamentável o legado de contaminação que o desastre causou para as pessoas que viviam no seu entorno. Até hoje boa parte da região atingida tem seu acesso controlado e até mesmo viver na região é proibido. Outrossim, o desastre de Chernobyl trouxe à discussão o questionamento sobre os valores inerentes ao processo de informação sobre os riscos das novas tecnologias e o quanto ele deve ser transparente, justo e conhecido. Além disso, ele foi outro palco, assim como Bophal, de ações mitigatórias e protocolos de resposta ineficientes, demoradas e sem transparência.

- **Fukushima – 2011:** Em 11 de março de 2011, a usina nuclear de Fukushima teve três dos seus 6 reatores nucleares colapsados, liberando significativa quantidade de radiação.

O desastre de Fukushima tem uma de suas causas relacionadas a um tsunami que atingiu a usina. Por isso é possível encontrar definições que colocam esse desastre como tendo origens mistas. Definido, como citado anteriormente, eventos naturais que desencadeiam um desastre tecnológico. No entanto, baseando-se na classificação brasileira de desastres, enquadraríamos como desastre tecnológico.

O caso de Fukushima nos apresenta mais uma característica fundamental para o entendimento da gestão de riscos de desastres tecnológicos: a confiança, até certo ponto, cega frente aos pareceres de peritos e técnicos. Embora todos os casos citados contassem com pareceres de peritos acerca dos riscos, esse em especial e nesse aspecto, tem maior significado que os demais. Além de ser muito contemporâneo, atingiu um dos países com a maior capacidade tecnológica do globo, até mesmo referência para a gestão de desastres. Mostra-nos, desta forma, que mesmo os peritos baseados em complexos estudos podem falhar e propiciar condições para emergência de grandes tragédias.

- **Brumadinho – 2019:** Em janeiro de 2019, no município de Brumadinho, Minas Gerais, rompe a barragem de rejeitos da mina Córrego do Feijão. Em consequência causou um dos maiores desastres tecnológicos brasileiros e um dos maiores rompimentos de barragem do mundo.

Muitas características desse desastre chamam atenção: suas consequências diretas e indiretas a vidas humanas e ao meio ambiente; a falta de investimentos em medidas de prevenção e gestão de riscos realmente efetivas; e, além das exigências puramente legais, que no caso em tela foram parcialmente cumpridas, até porque há inquéritos atestando laudos possivelmente manipulados que credenciavam a segurança do empreendimento; ou então a aparente incapacidade de aprender com desastres anteriores, já que a proprietária da barragem era uma das controladoras da barragem de Mariana, que rompeu em 05 de novembro de 2015, gerando um dos maiores impactos para o meio ambiente que, no Brasil, um desastre tecnológico já causou.

2.2 Os sistemas peritos

O conceito de sistemas peritos estabelecido por Anthony Giddens é de suma importância na busca de um entendimento mais claro sobre gestão de riscos de desastres tecnológicos, assim como da sua efetiva prática.

Antes de discorrer sobre os sistemas peritos e sua importância no processo de gestão de risco de desastre tecnológico, é fundamental entender o conceito de modernidade que, segundo Giddens, possibilita a construção do conceito. Giddens entende que o tempo que vivemos é marcado pela evolução que, se traz conforto e solução para problemas, adstritamente também cria novos riscos.

> A modernidade, como qualquer um que vive no final do século XX pode ver, é um fenômeno de dois gumes. O desenvolvimento das instituições sociais modernas e sua difusão em escala mundial criaram oportunidades bem maiores para os seres humanos gozarem de uma existência segura e gratificante que qualquer tipo de sistema pré-moderno. Mas a modernidade tem também um lado sombrio, que se tornou muito aparente no século atual. (GIDDENS, 1991, p. 17)

Outra característica marcante da modernidade, tal como definida por Giddens, é o desencaixe das relações sociais. Em outras palavras, antes da modernidade a nossa relação com espaço e tempo era completamente acoplada. Estávamos presos aos ciclos da natureza, havendo um respeito aos tempos biológicos e naturais, da mesma forma que as tradições pautavam nossas relações sociais. Com o advento da modernidade, afastamo-nos desses tipos de relação. Segundo Giddens (1991), as relações sociais se deslocaram dos contextos locais de interação mediante extensões indefinidas de tempo-espaço.

Por esta perspectiva interpretativa, dois tipos de mecanismos de desencaixe tem destaque: as fichas simbólicas e os sistemas peritos. As fichas simbólicas são, segundo Giddens (1991), *meios de intercâmbio que podem ser "circulados" sem ter em vista as características específicas dos indivíduos ou grupos que lidam com eles em qualquer conjuntura particular.* Um exemplo de fichas simbólicas é o dinheiro.

Já os sistemas peritos são definidos como:

> Por sistemas peritos quero me referir a sistemas de excelência técnica ou competência profissional que organizam grandes áreas dos ambientes material e social em que vivemos hoje. A maioria das pessoas leigas consulta "profissionais" – advogados, arquitetos, médicos etc. – apenas de modo periódico ou irregular. Mas os sistemas nos quais está integrado o conhecimento dos peritos influenciam muitos aspectos do que fazemos de uma maneira contínua. (GIDDENS, 1991, p. 38)

Os sistemas peritos tem relação direta com a confiança, uma vez que não podemos ser especialistas em tudo e nem dispomos de tempo suficiente para alcançar co-

nhecimento sobre tudo que nos cerca. Temos invariavelmente que depositar nossa confiança em peritos. Isso se aplica a quase tudo em nossa vida moderna, das rotinas mais triviais como, por exemplo: viver em um prédio confiando que ele não vá colapsar; ou então quando dirigimos eventualmente nossos carros acreditando que, quando o freio for acionado, ele fará o carro parar; e até exemplos mais complexos como a confiança que um avião não vá cair em pleno voo.

Onde existem lacunas de conhecimento, invariavelmente, há confiança; e essa confiança não é conquistada por um encontro direto com o perito que atesta a segurança de um determinado sistema. Confiamos no sistema independente de conhecermos as pessoas nele envolvidas.

Os sistemas peritos assumem os riscos para os leigos, mas nem sempre são evidentes e possíveis para o leigo identificar a real proporção deste risco, seja em termos de probabilidade ou impacto. Outras vezes os sistemas peritos nem transparecem a real existência de um determinado risco, seja pela necessidade de camuflar para não causar pânico e inviabilizar economicamente um negócio, ou até mesmo pelo desconhecimento por parte dos próprios peritos quanto a certo risco.

> Os peritos frequentemente assumem riscos "a serviço" dos clientes leigos, embora escondam ou camuflem a verdadeira natureza desses riscos, ou mesmo o fato de existirem riscos. Mais danoso que a descoberta por parte do leigo deste tipo de ocultamento é a circunstância em que a plena extensão de um determinado conjunto de perigos e dos riscos a eles associados não é percebida pelos peritos. (GIDDENS, 1991, p. 144)

Portanto, os desastres tecnológicos podem ser entendidos como a concretização da falha de um sistema perito. Essa falha se dá pela materialização do risco que era gerenciado. Quando conhecido pelo sistema, ele se manifesta de duas formas básicas: defeito no projeto ou falha do operador. Esses efeitos compõem o que Giddens chama de consequências inesperadas.

> Não importa o quão bem um sistema é projetado nem o quão eficientes são seus operadores, as consequências de sua introdução e funcionamento, no contexto da operação de outros sistemas e da atividade humana em geral, não podem ser inteiramente previstas. Uma razão para isto é a complexidade dos sistemas e ações que constituem a sociedade. (GIDDENS, 1991, p. 167)

O conceito que define um sistema perito e suas inerentes deficiências, em razão da impossibilidade de prever todas os potenciais inesperados relacionados a um defeito no projeto ou então à falha de um operador, torna evidente a necessidade de uma gestão independente e participativa de riscos de desastres tecnológicos. Não por uma estrutu-

ra interna, atrelada ao processo de atenuação característico do sistema perito que tem por interesse primário, perpetuar um negócio em detrimento das reais possibilidades de risco; e principalmente das reais consequências que esses riscos podem ter sobre as pessoas a ele expostas. Gerir o risco tecnológico produzido por meio do desenvolvimento de processos econômicos de negócio implica claro conflito de interesses, principalmente em países onde há subterfúgios legais disponíveis, assim como a proteção que a pessoa jurídica, que não é uma pessoa de fato, fornece à pessoa física que aceita o risco em nome da coletividade, todavia exposta as consequências de sua concretização.

2.3 Benefício privado e risco coletivo

Uma característica comum aos riscos de desastre tecnológicos e que precisa ser discutida incide sobre o reconhecimento de uma real preocupação com a prevenção e a mitigação de tais riscos, quando consideramos o caráter público das consequências que esses riscos têm a partir de decisões privadas e unilaterais. Em outras palavras, instituições que potencialmente são geradoras de riscos de desastre tecnológico tomam decisões internas e privadas – sem participação efetiva de *stakeholders* – em relação à prevenção e/ou mitigação de determinados riscos que, caso sejam concretizados, terão consequências para toda uma coletividade, em danos humanos, físicos ou ambientais.

A aceitação desta lógica decisória, em boa parte é explicada pelo conceito de sistemas peritos abordado anteriormente. Como não podemos ser especialistas em tudo e nem temos a capacidade de verificar a confiabilidade de tudo, depositamos nossa confiança em empresas especialistas no assunto que, em teoria, detêm um corpo técnico e imparcial capaz de adotar medidas mais seguras em relação aos riscos. Não há dúvida que diversas instituições geradoras de riscos valem-se dessa lógica para assumir riscos que impactam a coletividade, tanto economizando em medidas de segurança como atendendo, quando muito, o mínimo exigido em lei e usando de sua capacidade de comunicação para minimizar os riscos e mostrar o que interessa aos *stakeholders*.

Ao observar desastres tecnológicos como, por exemplo, o caso de Brumadinho, reconhecemos que os maiores afetados são pessoas que não tomaram a decisão que criou o risco e nem lucravam com esse risco.

Outro fator que também chama a atenção sobre esse processo privado de decisão sobre riscos de desastre tecnológico, é o evidente conflito de interesses intrínsecos a quem gera o risco e tem que comunicá-lo aos potenciais afetados, sem impactar o seu negócio. Para entendermos melhor esse ponto, basta usarmos como exemplo os casos dos rompimentos de barragem de Mariana, em 2015, e a barragem de Brumadinho, rompida em 2019. Ambas as barragens eram classificadas como de baixo risco, embora

tivessem o que no sistema de classificação da Agência Nacional de Mineração (ANM) é chamado de dano potencial associado (DPO) alto. Nos dois casos, havia uma exploração econômica das barragens. Portanto, custos eram acompanhados e administrados com o intuito de buscar o máximo benefício com o mínimo dispêndio financeiro. Essa máxima é comum a toda e qualquer gestão empresarial e financeira. Por si só, não é um erro, pois evita desperdício, fator importante nos cálculos de sustentabilidade. No entanto, quando lidamos com a possibilidade de um desastre que tem potencial de destruição alto, a máxima da otimização de custos só pode ser alcançada depois que todo investimento possível para a segurança for adotado. A forma como operavam as barragens, assim como as ações de prevenção e mitigação observadas nos dois desastres deixam claro que não havia o cuidado máximo com a segurança. Essa tese é facilmente reforçada se observarmos o método de construção que foi adotado no caso das duas barragens. Em ambas se optou pelo processo de alteamento à montante, que é a forma mais barata e também mais insegura de construção de barragens. Ou seja, há um claro conflito de interesse entre a otimização econômica da exploração da barragem e o máximo cuidado possível com a segurança das pessoas expostas ao risco de um rompimento da estrutura.

> A legislação brasileira de barragens (lei nº 12.334, de 20 de setembro de 2010) estabelece que é responsabilidade do empreendedor garantir a segurança de suas estruturas e que a fiscalização das atividades de mineração é compartilhada entre a Agência Nacional de Mineração (ANM) e os órgãos ambientais licenciadores estaduais. O cadastramento é realizado com o fornecimento unilateral de informações pela empresa. Ocorre que essa mesma declaração de risco é usada para determinar quais estruturas terão prioridades na fiscalização, criando a possibilidade de distorção dos fatos por empresas que queiram evitar a fiscalização. (FREITAS; SILVA, 2019, p. 25)

A decisão de como construir as barragens de Mariana e de Brumadinho, no exemplo citado anteriormente ratifica o quão perigoso é a concentração privada da decisão de um risco coletivo. Muito provavelmente, se houvesse clareza na comunicação dos riscos envolvidos e nas ações tomadas para preveni-los e mitigá-los teríamos um resultado diferente daquele que os dois desastres geraram. Mais uma vez faz-se necessário valer-se de interpretações de Beck, para entender que muitos riscos de desastres tecnológicos estão baseados em estruturas de poder que impõe danos a pessoas sem a chance de elas poderem participar do processo decisório.

> A estrutura de poder do risco está fundada na lógica do risco. Este pressupõe uma decisão, e, portanto, alguém que toma a decisão, o que produz uma assimetria radical entre aqueles que decidem, definem e tiram proveito dos riscos e aqueles que são seus alvos, que sofrerão diretamente os "efeitos colaterais imperceptíveis" das

> decisões de outros, que talvez tenham até mesmo de pagar por elas com suas próprias vidas, sem poder fazer parte do processo decisório. (BECK, 2011, p. 366)

Em síntese, riscos coletivos devem ter participação coletiva nos processos de prevenção e mitigação, mesmo que isso implique na inviabilidade de certos projetos. A busca para uma justa e eficaz gestão de riscos de desastres tecnológicos deve passar obrigatoriamente pela participação de todos os *stakeholders*, principalmente os mais vulneráveis e atingidos diretamente pela eventual concretização do risco, possibilitando o debate e a exposição do contraditório. Riscos coletivos devem invariavelmente contar com decisões coletivas.

3. GOVERNANÇA DO RISCO, UMA ALTERNATIVA

Desastres tecnológicos, normalmente, trazem grandes consequências para a sociedade, fato esse ilustrado ao longo do artigo.

Também podemos evidenciar, por meio dos exemplos, que a gestão de risco de desastre tecnológico não é algo compartilhado efetivamente com as partes interessadas, principalmente com os atingidos pelas consequências. Quando muito, essa parcela de pessoas é comunicada sobre os riscos a que se encontra exposta, mas sempre de forma sútil e enviesada, visando atenuar um potencial problema envolvendo a insatisfação e/ou preocupação das pessoas e a organização geradora do risco. Muito desse processo, como vimos, se dá através da confiança nos sistemas peritos.

Essa ausência da participação das partes interessadas (*stakehokders*) pode ser resultado da inexistência formal de uma etapa do processo de gestão de riscos que contemple, de maneira efetiva, a gestão de preocupações dos *stakeholders*. Vale destacar que a efetiva participação dos *stakeholders*, notadamente os potenciais atingidos, não deve ser entendida simplesmente como um chamamento público para esclarecimentos unilaterais quanto ao risco e quanto as medidas de contingência, adotadas pela organização geradora do risco, mas sem a possibilidade de contraditório. Ações dessa natureza podem estar travestidas de um processo participativo, mas não passam de um processo informativo, ou seja, é desenvolvido e conduzido unicamente para dar ciência da existência do risco e, mais do que isso, para comunicar que as probabilidades de um desastre, de acordo com os peritos da organização que gera o risco, são quase nulas. Nenhum dos potenciais atingidos é questionado se está disposto a correr esse risco, não são apresentadas linhas de pesquisa conflitantes sobre esse risco para uma discussão, não há benefícios oferecidos para a aceitação desse risco, assim como não são detalhadas todas as formas possíveis de tratar esse risco para que haja uma deliberação sobre o melhor

tratamento a se dar. O risco é gerado, tratado e algumas vezes comunicado aos atingidos que pouco ou nada podem fazer. Os únicos interesses levados em consideração nesse processo de gestão de riscos são os interesses de quem gera o risco.

> As estratégias de comunicação de risco baseadas nesse modelo se mostraram ineficazes, uma vez que não engajavam o público nos debates sobre riscos, não consideravam suas perspectivas e focavam somente na transmissão da informação dos peritos para os "leigos", como se o objetivo da comunicação de risco fosse exclusivamente o de educar e convencer o público. (DI GIULIO *et al*., 2010, p. 286)

Entendemos que para que haja um eficaz processo de gestão de riscos de desastres tecnológicos deve-se haver um processo participativo, envolvendo todos *stakeholders,* principalmente aqueles que são impactados diretamente pelo eventual desastre. Adotar uma abordagem unilateral invariavelmente pode conduzir a um processo injusto, visto que somente uma parte dos interesses é contemplada, fazendo assim com que o risco seja tratado unicamente sob a ótica do gerador do risco que, evidentemente, também sofre as consequências, mas que é o único que tem benefícios com as decisões tomadas em relação e esse risco.

> A abertura do diálogo e do processo decisório implica o reconhecimento de que a comunicação de risco não deve se limitar ao modelo do déficit de conhecimento, no qual os peritos comunicam os conhecimentos e suas verdades científicas para os leigos para evitar que estes permaneçam na ignorância e irracionalidade. (DI GIULIO *et al*., 2010, p. 238)

Um dos grandes desafios para essa efetiva gestão do risco de desastra tecnológico está na mudança do modelo adotado habitualmente que pode ser definido como *modelo do déficit de conhecimento* (DI GIULIO *et al*., 2010) para um modelo de múltiplos conhecimentos e principalmente múltiplas preocupações. O conhecimento leigo pode, em alguns casos, não ter tanta relevância em se tratando de riscos tecnológicos diferentemente do que acontece com os riscos naturais que muitas vezes é requerido e explorado, mas entender as preocupações que consternam as pessoas que potencialmente sofreriam as consequências de um desastre tecnológico é a primeira etapa para buscar um tratamento que antes de ser viável economicamente, seja justo socialmente para todos.

3.1 A estrutura do processo de Governança do risco

Uma proposta de abordagem para a gestão de riscos que contemple a participação mais ativa dos *stakeholders* e que busque por uma distribuição mais igualitária de riscos e benefícios, pode ser uma alternativa aos modelos adotados regularmente pe-

las organizações geradoras de riscos de desastre tecnológicos pode estar no modelo de gestão de riscos proposto pelo *International Risk Governance Council* (IRGC). Esse modelo parte do princípio da governança de risco, conceito esse definido por eles como:

> Risk governance applies the principles of governance to the identification, assessment, management, evaluation and communication of risks in the context of plural values and distributed authority, it includes all important actors involved, considering their rules, conventions and processes. It is thus concerned with how relevant risk information is collected, analyzed, understood and communicated, and how management decisions are taken and communicated. Risk governance mobilizes both descriptive issues (how decisions are made) as well as normative concepts (how decisions should be made). In its application as a normative concept it specifies the principles of good governance. These principles include transparency, effectiveness and efficiency, accountability, strategic focus, sustainability, equity and fairness, respect for the rule of law, and the need for the chosen solution to be politically and legally feasible as well as ethically and publicly acceptable. (IRGC, 2017, p. 5)

Esse tipo de abordagem pressupõe maior participação de todos os *stakeholders* envolvidos e afetados pelo potencial risco. Buscando dessa forma alcançar um processo de gestão de riscos mais justo, onde todos possam gozar dos benefícios e reparações, assim como estar cientes dos ônus que determinadas escolhas podem gerar.

A estrutura básica de gestão de riscos adotada pelo IRGC é composta pelas cinco etapas descritas a seguir:

1. Pré-avaliação

É o processo inicial onde a organização busca identificar os riscos, assim como os *stakeholders* a eles relacionados.

A pré-avaliação tenta esclarecer as várias perspectivas que o risco pode implicar, levando em conta a multiplicidade de questões que os *stakeholders* e a organização podem associar a esse determinado evento.

Nessa primeira etapa do processo de gestão de riscos proposto pelo IRGC, já é possível notar a particularidade da preocupação com a visão que as partes interessadas têm sobre o processo de gestão de riscos. Além de identificar quem são os *stakeholders*, há a busca pelas perspectivas que eles têm acerca do risco. Portanto, parte se do princípio de que o *stakeholder* não é um mero observador, referenciado por um déficit de conhecimento, mas sim alguém que pode e deve contribuir para o processo de gestão de riscos.

2. Análise

A etapa de análise proposta pelo IRGC é composta por dois tipos de avaliação, uma convencional, onde o risco é o protagonista, e outra onde as preocupações dos *stakeholders* são o principal foco. Nesse ponto, podemos destacar mais uma grande diferença entre o processo de gestão de riscos proposto pelo IRGC em relação ao processo convencional. No modelo proposto pela IRGC, como etapa formal do processo de gestão de riscos, há que se fazer uma avaliação de preocupações de *stakeholders*.

3. Caracterização e avaliação

Nessa etapa do processo de gestão de riscos, os resultados obtidos com a análise anterior (das avaliações de riscos e de preocupações) são comparados com critérios pré-estabelecidos pelos responsáveis em conduzir o processo de gestão de riscos. Tudo isso a fim de determinar a aceitabilidade do risco e a fundamentação para a tomada de decisão relativa aos futuros tratamentos que, porventura, podem ser dados aos riscos.

Durante essa etapa, segundo o modelo adotado pelo IRGC, o risco é caracterizado como simples, complexo, incerto, ambíguo, ou como combinação desses tipos.

Simples – riscos que bastam regulações simples para obter resultados positivos no seu gerenciamento. Um exemplo é a utilização do cinto de segurança quando dirigindo um veículo, a fim de atenuar as consequências de uma eventual colisão.

Complexo – se refere aos riscos onde há dificuldade na identificação e quantificação das causas, assim como em todos as consequências possíveis. Um exemplo pode ser a interrupção de uma infraestrutura de fornecimento de internet.

Incerto – se refere à falta de dados científicos sobre determinada tecnologia ou circunstância. Um exemplo pode ser o desenvolvimento de novos organismos por meio de biotecnologia e da inserção deles no meio natural.

Ambíguo – refere-se a riscos com perspectivas divergentes, por suas consequências ou probabilidades de ocorrência. Normalmente são os riscos que envolvem um conflito entre questões éticas e ganhos econômicos.

Nessa etapa há ainda a definição quanto à aceitabilidade do risco, a partir da combinação das avaliações de risco e preocupações. O resultado deste procedimento gera três formas de entendimento do risco:

- Risco aceitável – quando as medidas de redução do risco são desnecessárias.
- Risco tolerável – quando o risco pode ser aceito, mas sujeito a medidas apropriadas de redução.
- Risco intolerável – quando nenhuma medida de redução consegue tornar o risco tolerável.

4. Gerenciamento

Esta etapa envolve o desenvolvimento, a implementação e a revisão de soluções para o tratamento dos riscos analisados e caracterizados na fase anterior. Buscam-se as opções mais eficientes para lidar com a complexidade, incerteza e ambiguidade dos riscos.

5. Aspectos transversais

As quatro etapas citadas anteriormente acontecem de forma cíclicas, uma após a outra; e permeando todas essas etapas, existe o que o IRGC denomina como aspectos transversais, ou seja, aspectos que ao longo de cada uma das fases são considerados no processo de governança do risco. Esses aspectos são: a comunicação, o engajamento de *stakeholders* e a importância do contexto.

Comunicação – é o processo de troca de informações que acontece em cada uma das fases, entre os diversos *stakeholders*. Esse processo auxilia os gestores de riscos a entender suas tarefas e responsabilidades, assim como capacita os *stakeholders* no entendimento dos riscos e no seu processo de gerenciamento.

Engajamento de *stakeholders* – é o processo de envolver todas as partes interessadas durante as fases do processo. Isso tem como objetivo melhorar a relevância da decisão, assim como o desempenho dos resultados esperados. Envolver *stakeholders* torna o processo de gestão de riscos inclusivo, participativo, além de ajudar na imparcialidade do processo e ajudar as organizações geradoras do risco a identificarem preocupações que, muitas vezes, não fazem parte do escopo inicial dos riscos identificados.

A importância do contexto – é a enfase que deve ser dada à compreensão dos contextos sociais, institucionais, políticos e econômicos de onde o processo de gestão de riscos é conduzido e ao logo de cada etapa do processo, principalmente na tomada de decisões.

Quanto à participação das pessoas diretamente atingidas pelo desastre no processo de gestão de riscos, cabe destacar que, no campo dos desastres naturais, essa participação é mais frequente que na gestão de riscos de desastres tecnológicos. Talvez

o motivo de tal diferença esteja relacionado com a fonte geradora do risco, uma vez que, de maneira geral, os riscos naturais, como o próprio nome diz, tem sua fonte em eventos naturais. Não há quem tire proveito econômico de tal risco, logo não há conflito de interesses envolvendo afetados. Já com os desastres tecnológicos, há uma participação direta de organizações que lucram na produção desse risco, fazendo com que não seja interessante envolver afetados que não se beneficiam do risco na discussão de meios para geri-lo, pois isso ensejaria maior preocupação com as probabilidades e consequências desse risco. Podendo, desta forma, comprometer o desenvolvimento econômico da organização criadora do risco, havendo assim um claro conflito de interesse na participação de *stakeholders* no processo de gestão de riscos de desastres tecnológicos.

Outrossim, cabe ressaltar que o modelo descrito, com certeza, está longe da perfeição. Entretanto pode ser um caminho para alcançarmos um processo de gestão de riscos de desastre tecnológico mais eficaz no que tange à participação de *stakeholders*, compartilhamento de benefícios e riscos de forma equitativa e principalmente justo na decisão de como lidar com o risco.

4. CONSIDERAÇÕES FINAIS

A principal proposta deste trabalho foi trazer à luz uma alternativa ao modelo de gestão de riscos de desastres tecnológicos, comumente adotada pelas organizações que promovem tais riscos em decorrência de seus processos produtivos.

Como foi possível observar ao longo dos exemplos de desastres tecnológicos apresentados, os maiores afetados pela concretização de tais fenômenos normalmente têm pouco conhecimento de sua existência; assim como não participam de qualquer processo decisório quanto ao tratamento dos riscos aos quais estão expostos.

A implementação de modelos de gestão de riscos de desastre tecnológicos participativos não busca apenas facilitar o diálogo entre quem gera o risco e quem está a ele exposto. Constitui um processo pelo qual haja a possibilidade de escolha entre como tratar aquela potencialidade, não somente analisando a medida mais econômica para a organização geradora do risco.

Refletindo sobre os exemplos citados, notadamente o recente caso nacional relacionado ao rompimento da barragem de Brumadinho – MG, é possível afirmar que há, ainda, um longo caminho a ser percorrido em busca da implementação do justo modelo de gestão de riscos de desastre, participativo e pautado prioritariamente na preservação da vida. O desafio tem início na própria discussão do tema que, mesmo no meio acadê-

mico nacional, ainda é muito incipiente, os desastres naturais são muito mais valorados e pesquisados.

Outro fator que reforça a magnitude do desafio decorre de não termos a menção do termo desastre tecnológico em nossa Política Nacional de Proteção e Defesa civil, publicada em 10 de abril de 2012. Notadamente, a lei número 12.608/12 deu maior importância aos desastres oriundos dos riscos naturais, notadamente os eventos geológicos e climáticos, assim como a ocupação do solo, muito provavelmente por serem riscos que, no Brasil se concretizam com grande frequência em determinadas épocas do ano.

Entendemos que melhorar o processo de gestão de riscos de desastres tecnológicos consiste na incorporação de dimensões subjetivas representadas pela avaliação de preocupações, etapa proposta pelo modelo estabelecido pelo IRGC; e não só a manutenção do modelo técnico objetivo, conduzido unilateralmente pela organização geradora de riscos. Incluir a participação de *stakeholders* no processo decisório da gestão de riscos de desastres tecnológicos tende, consequentemente ao desenvolvimento de um processo de cobrança, além de maiores medidas de controle, assim como a possibilidade do esclarecimento real quanto às consequências que a concretização dos riscos pode gerar e garantir uma percepção de riscos adequada ao cenário existente.

Cabe ressaltar que não pretendemos, com isso, afirmar que modelos de gestão de riscos objetivos não exercem importante papel, ou têm papel diminuto no processo. Todavia a busca por soluções para uma efetiva e eficaz gestão de riscos de desastres tecnológicos necessita de abordagem ampla, levando em consideração não só os interesses da organização geradora de riscos, mas os interesses dos eventuais atingidos.

Também identificamos que modelo de governança do risco encontra uma limitação quando não é possível identificar, com clareza, os potenciais atingidos pelo desastre tecnológico, como é o caso de determinados incêndios urbanos. Nesses casos e algumas vezes, as vítimas ocupam a instalação atingida pela tragédia de forma transitória e temporária. Não se torna possível, dessa forma, estabelecer uma avaliação de preocupações efetivas. Um exemplo específico é o desastre tecnológico do incêndio urbano ocorrido na boate *Kiss* em Santa Maria – RS, em 27 de janeiro de 2013, episódio que causou a morte de 242 pessoas.

Concebemos que não há gestão de riscos de desastre tecnológico capaz de contemplar todas as incertezas envolvidas nos processos desenvolvidos pela sociedade. No entanto, a busca por um processo que priorize a vida e a participação dos potencialmente atingidos, antes de qualquer outro interesse, é possível e viável.

Por fim, gostaríamos de compartilhar as palavras do filósofo francês Émile-Auguste Chartier, citadas no livro "Renovação Radical" de Henry Mintzberg: "Toda mu-

dança parece impossível, mas uma vez realizada, é o estado em que já não estamos mais que parece impossível".

REFERÊNCIAS BIBLIOGRÁFICAS

ALEKSIÉVITCH, S. **Vozes de Tchernóbil**: a história oral do desastre nuclear. São Paulo: Companhia das Letras, 2016.

BECK, U. **Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Editora 34, 2010.

BRASIL. Lei nº 12.608, de 10 de abril de 2012. Institui a Política Nacional de Proteção e Defesa Civil - PNPDEC; dispõe sobre o Sistema Nacional de Proteção e Defesa Civil - SINPDEC e o Conselho Nacional de Proteção e Defesa Civil - CONPDEC; autoriza a criação de sistema de informações e monitoramento de desastres; altera as Leis nos 12.340, de 1o de dezembro de 2010, 10.257, de 10 de julho de 2001, 6.766, de 19 de dezembro de 1979, 8.239, de 4 de outubro de 1991, e 9.394, de 20 de dezembro de 1996; e dá outras providências. **Diário Oficial da União**, Brasília, 11 abr. 2012.

CASTRO, A. L. C. **Glossário de Defesa Civil, estudos de riscos e medicina de desastres**. Brasília: Ministério da Integração Nacional, 2009.

DI GIULIO, G. M.; FERREIRA, L. C.; FIGUEIREDO, B. R.; DOS ANJOS, J. A. S. A. Comunicação e governança do risco: a experiência brasileira em áreas contaminadas por chumbo. **Ambiente e sociedade**, v. XIII, n. 2, p. 283-297, 2010.

FREITAS, C. M.; BARCELLOS, C.; ASMUS, C. I. R. F.; SILVA, M. A.; XAVIER, D. R. Da Samarco em Mariana à Vale em Brumadinho: desastres em barragens de mineração e saúde coletiva. **Cadernos de Saúde Pública**, 2019.

GIDDENS, A. **As consequências da modernidade**. São Paulo: Editora Unesp, 1991.

IRGC. **Introduction to the IRGC Risk Governance Framework**. Revised version. Lausanne: EPFL International Risk Governance Center, 2017.

MARTINS, B. S. Revisitando Bhopal: os tempos da violência e as latitudes da memória. **Sociologias**, p.116-148, 2016.

MINTZBERG, H. **Renovação radical**: uma estratégia para restaurar o equilíbrio e salvar a humanidade e o planeta. Porto Alegre: Bookman Editora LTDA, 2015.

PEREZ, R. C. **Emergências tecnológicas**. Sorocaba: Editora Cidade, 2016.

UNDRR. **Termonology**. Disponível em: https://www.undrr.org/terminology/disaster#:~:text=A%20serious%20disruption%20of%20the,and%20environmental%20losses%20and%20impacts. Acesso em: 18 nov. 2020.