

# Sugestões para debate e avaliação da comissão, relativo ao Marco Regulatório da Inteligência Artificial (Prof. F.Osório - USP)

Fernando Santos Osorio <fosorio@usp.br>

sex 10/06/2022 21:51

Para:CJSUBIA <CJSUBIA@senado.leg.br>;

Cc:Fernando Santos Osorio <fosorio@icmc.usp.br>;

 2 anexos

Marco-Regulatorio-IA--Dr-Fernando-Osorio-USP.docx; Marco-Regulatorio-IA--Dr-Fernando-Osorio-USP.pdf;

Você não costuma receber emails de fosorio@usp.br. [Saiba por que isso é importante](#)

Prezado Sr.(a):

O texto que segue abaixo (no corpo desta mensagem) é o mesmo contido nos anexos (em formato .docx e .pdf).

Atenciosamente,

Prof. Dr. Fernando Santos Osório - USP/ICMC

Curruculum CV Lattes: <http://lattes.cnpq.br/7396818382676736>

Linkedin: <https://www.linkedin.com/in/fernando-osorio-usp/>

USP: <https://www.icmc.usp.br/pessoas?id=10438287>

=====

São Carlos, SP – 10 de junho de 2022

**De: Prof. Dr. Fernando Santos Osório – USP / ICMC** (Universidade de São Paulo)

Professor e Pesquisador da USP São Carlos - ICMC – Inst. de Ciências Matem. e da Computação

Membro do Conselho Executivo do Centro de Inteligência Artificial – C4AI – USP+IBM+FAPESP

Membro do Comitê Gestor do Centro de Robótica da USP – CRob/USP – São Carlos

**Para:** Comissão de Justiça do Senado – Subcomitê do Marco de Regulamentação da IA (CJSUBIA)

E-mail: [cjsubia@senado.leg.br](mailto:cjsubia@senado.leg.br)

Prezado Sr.(a),

Venho por meio desta encaminhar uma lista de sugestões para debate e avaliação relativo ao **Marco Regulatório da Inteligência Artificial**, junto a Comissão de Justiça do Senado Federal, que trata deste assunto. Envio este documento, como (minhas) sugestões externas, conforme solicitado pelo próprio comitê – CJSUBIA. Ressalto que tais opiniões e sugestões refletem minha experiência de mais de 30 anos de ensino e pesquisas na área de Inteligência Artificial, área de minha formação no Mestrado e Doutorado (Título de Doutor obtido na França). Esse tema é bastante sensível, e controverso, onde não posso garantir que haja um consenso geral das entidades as quais estou ligado (USP, C4AI e CRob/USP), porém são posições que refletem a opinião de muitos dos pesquisadores da área.

## Referente aos Veículos Inteligentes e Autônomos:

1. Todo veículo dotado de sistemas de apoio ao motorista, e de atuação/ação junto a condução dos veículos, deve ser dotado de uma “**caixa preta**” (*data logger*), nos moldes do que é adotado em aviões, que possuem “pilotos automáticos” e instrumentos de navegação.

Os veículos que possuem sensores podem e DEVEM registrar os dados (“log”), para fins de auditoria em caso de acidentes que causem danos materiais ou às pessoas (impactando a responsabilidade civil e penal em caso de

acidentes e cobertura de seguros). A caixa preta permite identificar o “responsável” pela falha: componente, software/hardware, fabricante do veículo, condutor/proprietário, passageiros, e mesmo elementos externos).

1.1. Deve ser bem definida a classe destes sistemas que irão registrar os dados, pois não somente os veículos autônomos (“*fully autonomous*”) devem ser dotados de sistemas de aquisição e registro de dados (caixas pretas/*data loggers*). Devem ser definidas categorias de dados NECESSÁRIOS para constar no registro, conforme o tipo de veículo, de sensores disponíveis e adotados, e do nível de autonomia do veículo (*SAE's automation level definitions*). Retomo aqui o exemplo dos aviões, onde alguns possuem só registro de rota, ou de voz, e os mais avançados possuem um registro mais completo (mais de uma caixa preta) – Sistemas que se baseiam em câmeras, devem registrar dados das câmeras, se usam radares, devem registrar os dados dos radares, se atuam na direção e freios, os dados dos mesmos, e assim por diante.

1.2. Deve haver uma entidade ISENTA que tenha acesso a estes dados em caso de avaliação de responsabilidades e de acidentes. Não deve ser o próprio fabricante o único e principal responsável pela avaliação de falhas e acidentes. Por exemplo, no caso de aviões, quem é responsável por investigações é a CENIPA, órgão com maior isenção em investigações de acidentes aéreos.

1.3. Deve se prezar pela TRANSPARÊNCIA nos dados dos veículos, em caso de falhas e acidentes, visando permitir auditar o ocorrido. Além dos dados dos sensores, é necessário que a fabricante e responsáveis pelos softwares, no caso de uso de ferramentas de aprendizado de máquina, possuam código e dados de treino armazenados e passíveis de serem disponibilizados para a investigação da falha/acidente (salvar dados de treinamento do mecanismo inteligente do carro, que devem ser disponibilizados em caso de investigação)

1.4. Deve ser criada, de modo urgente, uma legislação para o controle e autorização de veículos de teste. O CTB (Código Brasileiro de Trânsito) não permite atualmente que existam carros experimentais em circulação. Com isso o Brasil vai ficar atrasado em suas pesquisas e desenvolvimentos em relação a outros países – A proibição atual de ter carros automatizados circulando, impede que maiores avanços sejam feitos nesta área.

1.5. Insisto para que sejam feitos estudos sobre as diferentes categorias de veículos automatizados, quanto ao nível de automação, quanto ao porte do veículo, quanto a sua circulação (p.ex. urbana, rodovias, estradas, rural), quanto ao risco que apresentam (p.ex. transporte coletivo de passageiros, transporte de carga, veículos pessoais) e quanto aos dados que obrigatoriamente cada um deles deve coletar e armazenar (“logs”).

1.6. E considero uma REGRA de OURO: todo veículo deve SEMPRE ter um condutor DENTRO do veículo pronto a assumir o volante. Pelo menos nesta fase de transição para uma geração mais “robusta” de veículos autônomos. Sendo mais preciso sobre a questão:

- Taxis autônomos não devem ser completamente autônomos (sem nenhum humano CAPACITADO em seu interior). Uma pessoa idosa não pode ficar sozinha dentro de um carro sem nenhuma assistência local humana;

- Caminhões e ônibus não podem circular sem um condutor humano, dentro do veículo, capacitado e pronto a intervir em situações de risco.

Esta regra considera o que ocorre atualmente com os aviões: eles até podem ser capazes de voar sozinhos, mas sempre possui uma equipe de bordo, capacitada e pronta a intervir em diferentes situações.

(\*) Em nosso laboratório de pesquisas (LRM – ICMC – USP) é completamente proibido experimentos com veículos em modo autônomo sem uma pessoa DENTRO do veículo.

## Referente a Robótica:

Um robô não pode JAMAIS decidir sobre a vida ou morte de uma pessoa. O Brasil deve ratificar as moções da ONU e de diferentes organismos internacionais sobre “robôs que matam”. Mesmo robôs militares não PODEM de modo algum decidir sozinhos se vão matar pessoas. Qualquer decisão, mesmo em situação de guerra, tem que ter um responsável pela decisão e ação, que poderá depois ser julgado pelas suas decisões, ações e ordens dadas.

➤ Este movimento é conhecido como: “*Stop Killer Robots*” ( <https://www.stopkillerrobots.org/> )

➤ Referências adicionais:

<https://www.hrw.org/topic/arms/killer-robots> Human Rights Watch

[https://en.wikipedia.org/wiki/Campaign\\_to\\_Stop\\_Killer\\_Robots](https://en.wikipedia.org/wiki/Campaign_to_Stop_Killer_Robots)

<https://www.reuters.com/world/un-chief-urges-action-killer-robots-geneva-talks-open-2021-12-13/>

<https://www.stopkillerrobots.org/news/unban/>

Uma máquina não pode ter o poder de decisão sobre a vida e a morte de uma pessoa. Nunca!

(\*) Mesmo os “drones” militares dos USA são controlados remotamente, e a decisão de atacar é humana.

## Referente aos Sistemas Inteligentes:

1. Todo sistema inteligente que utilize aprendizado de máquina (*machine learning*) deve ser transparente e auditável, ou seja, devem ser “armazenados” todos os dados e programas usados para colocar um determinado

sistema de Inteligência Artificial, baseado em aprendizado, em produção. Em caso de processos, danos, e da necessidade de uma auditoria externa, deve ser possível para os órgãos responsáveis pela investigação (a serem definidos em legislação própria para tal), que tenham acesso a estes dados.

Por exemplo, um sistema de diagnóstico médico baseado em Inteligência Artificial tem que ter os dados de treinamento (*datasets* e bases de aprendizado: dados “congelados” nas diferentes versões disponibilizadas para uso), armazenados e disponibilizados em caso de necessidade de uma auditoria e investigação sobre erros, falhas e danos causados pelo uso do sistema. Além dos dados, também é necessário que uma cópia do sistema seja armazenada e disponibilizada em caso de investigação (incluindo, por exemplo, redes de *deep learning* treinadas e usadas pelo sistema).

O objetivo desta “guarda de dados de treino e de sistemas” é poder avaliar o BIAS (tendências e desvios de comportamento) dos sistemas que possam ser prejudiciais aos usuários, com a identificação se existe alguma responsabilidade dos proprietários do sistema, pelo treino inadequado e pelas respostas do mesmo, que possam vir a causar danos a terceiros.

Os dados e programas que seriam auditáveis permanecem sigilosos, sendo apenas acessados pelos responsáveis da investigação, e que devem garantir que não haja vazamentos de dados.

Essa proposta visa criar sistemas AUDITÁVEIS, de modo a poder responsabilizar adequadamente aqueles que tenham alguma culpa/responsabilidade pelos danos causados pelos sistemas de I.A. Podemos fazer uma analogia com produtos farmacêuticos, onde a fórmula do remédio (composição) deve ser registrada, neste caso, a composição do sistema é composta pelos programas E TAMBÉM pelos dados usados para treinar a I.A. do sistema.

### Referente a Privacidade e o Respeito ao Indivíduo:

Acredito que devemos seguir o exemplo da LGPD (e a GDPR) no que diz respeito ao armazenamento e acesso a dados pessoais. Já existe uma legislação mais geral a esse respeito.

### Referente à Propriedade Intelectual:

Máquinas não são conscientes. Máquinas podem gerar informações de modo totalmente espontâneo e criativo. Máquinas geram “saídas” apenas quando uma pessoa fornece os dados de entrada e estimula o sistema a gerar um produto de saída. No meu entender, máquinas NÃO são proprietárias de obras literárias, musicais, ou, de arte (ou até mesmo patentes). O proprietário continua sendo o programador, ou, aquele que configura o sistema, ou, quem executa o sistema que leva a geração de uma obra: esse é o responsável, o proprietário, e quem deve responder legalmente pela obra criada (inclusive pode responder por plágios criados pela máquina). Tem que ter um responsável pelo produto final.

Assim como no caso dos robôs assassinos, ou, no caso das máquinas criativas, sempre deve haver uma pessoa responsável pela ação, pela criação, e que pode inclusive ser responsabilizada e processada pelos danos que venham a ser causados pela “sua máquina ou pelos atos da máquina”.

Agradeço a atenção dispensada, e espero ter contribuído para uma melhor regulamentação da I.A.,  
Prof. Dr. Fernando Santos Osório.

--

--

=====

Prof. Dr. Fernando Santos Osório - ICMC USP  
E-mail: fosorio .at. gmail. com or fosorio .at. ieee. org  
fosorio .at. usp. br - Office: (16) 3373.8174  
LRM Lab. / Center for Robotics CRob/USP-SC  
C4AI - Center for A.I.: <http://c4ai.inova.usp.br/>  
Homepage: <http://www.icmc.usp.br/~fosorio/>  
Research Group: <http://www.icmc.usp.br/~lrm/>

=====

São Carlos, SP – 10 de junho de 2022

**De: Prof. Dr. Fernando Santos Osório – USP / ICMC** (Universidade de São Paulo)

Professor e Pesquisador da USP São Carlos - ICMC – Inst. de Ciências Matem. e da Computação

Membro do Conselho Executivo do Centro de Inteligência Artificial – C4AI – USP+IBM+FAPESP

Membro do Comitê Gestor do Centro de Robótica da USP – CRob/USP – São Carlos

**Para:** Comissão de Justiça do Senado – Subcomitê do Marco de Regulamentação da IA (CJSUBIA)

E-mail: [cjsubia@senado.leg.br](mailto:cjsubia@senado.leg.br)

Prezado Sr.(a),

Venho por meio desta encaminhar uma lista de sugestões para debate e avaliação relativo ao **Marco Regulatório da Inteligência Artificial**, junto a Comissão de Justiça do Senado Federal, que trata deste assunto. Envio este documento, como (minhas) sugestões externas, conforme solicitado pelo próprio comitê – CJSUBIA. Ressalto que tais opiniões e sugestões refletem minha experiência de mais de 30 anos de ensino e pesquisas na área de Inteligência Artificial, área de minha formação no Mestrado e Doutorado (Título de Doutor obtido na França). Esse tema é bastante sensível, e controverso, onde não posso garantir que haja um consenso geral das entidades as quais estou ligado (USP, C4AI e CRob/USP), porém são posições que refletem a opinião de muitos dos pesquisadores da área.

#### **Referente aos Veículos Inteligentes e Autônomos:**

1. Todo veículo dotado de sistemas de apoio ao motorista, e de atuação/ação junto a condução dos veículos, deve ser dotado de uma “**caixa preta**” (*data logger*), nos moldes do que é adotado em aviões, que possuem “pilotos automáticos” e instrumentos de navegação. Os veículos que possuem sensores podem e DEVEM registrar os dados (“log”), para fins de auditoria em caso de acidentes que causem danos materiais ou às pessoas (impactando a responsabilidade civil e penal em caso de acidentes e cobertura de seguros). A caixa preta permite identifica o “responsável” pela falha: componente, software/hardware, fabricante do veículo, condutor/proprietário, passageiros, e mesmo elementos externos).
  - 1.1. Deve ser bem definida a classe destes sistemas que irão registrar os dados, pois não somente os veículos autônomos (“*fully autonomous*”) devem ser dotados de sistemas de aquisição e registro de dados (caixas pretas/*data loggers*). Devem ser definidas categorias de dados NECESSÁRIOS para constar no registro, conforme o tipo de veículo, de sensores disponíveis e adotados, e do nível de autonomia do veículo (*SAE's automation level definitions*). Retomo aqui o exemplo dos aviões, onde alguns possuem só registro de rota, ou de voz, e os mais avançados possuem um registro mais completo (mais de uma caixa preta) – Sistemas que se baseiam em câmeras, devem registrar dados das câmeras, se usam radares, devem registrar os dados dos radares, se atuam na direção e freios, os dados dos mesmos, e assim por diante.
  - 1.2. Deve haver uma entidade ISENTA que tenha acesso a estes dados em caso de avaliação de responsabilidades e de acidentes. Não deve ser o próprio fabricante o único e principal responsável pela avaliação de falhas e acidentes. Por exemplo, no caso de aviões, quem é responsável por investigações é a CENIPA, órgão com maior isenção em investigações de acidentes aéreos.

- 1.3. Deve se prezar pela TRANSPARÊNCIA nos dados dos veículos, em caso de falhas e acidentes, visando permitir auditar o ocorrido. Além dos dados dos sensores, é necessário que a fabricante e responsáveis pelos softwares, no caso de uso de ferramentas de aprendizado de máquina, possuam código e dados de treino armazenados e passíveis de serem disponibilizados para a investigação da falha/acidente (salvar dados de treinamento do mecanismo inteligente do carro, que devem ser disponibilizados em caso de investigação)
- 1.4. Deve ser criada, de modo urgente, uma legislação para o controle e autorização de veículos de teste. O CTB (Código Brasileiro de Trânsito) não permite atualmente que existam carros experimentais em circulação. Com isso o Brasil vai ficar atrasado em suas pesquisas e desenvolvimentos em relação a outros países – A proibição atual de ter carros automatizados circulando, impede que maiores avanços sejam feitos nesta área.
- 1.5. Insisto para que sejam feitos estudos sobre as diferentes categorias de veículos automatizados, quanto ao nível de automação, quanto ao porte do veículo, quanto a sua circulação (p.ex. urbana, rodovias, estradas, rural), quanto ao risco que apresentam (p.ex. transporte coletivo de passageiros, transporte de carga, veículos pessoais) e quanto aos dados que obrigatoriamente cada um deles deve coletar e armazenar (“logs”).
- 1.6. E considero uma REGRA de OURO: todo veículo deve SEMPRE ter um condutor DENTRO do veículo pronto a assumir o volante. Pelo menos nesta fase de transição para uma geração mais “robusta” de veículos autônomos. Sendo mais preciso sobre a questão:
  - Taxis autônomos não devem ser completamente autônomos (sem nenhum humano CAPACITADO em seu interior). Uma pessoa idosa não pode ficar sozinha dentro de um carro sem nenhuma assistência local humana;
  - Caminhões e ônibus não podem circular sem um condutor humano, dentro do veículo, capacitado e pronto a intervir em situações de risco.Esta regra considera o que ocorre atualmente com os aviões: eles até podem ser capazes de voar sozinhos, mas sempre possui uma equipe de bordo, capacitada e pronta a intervir em diferentes situações.

(\*) Em nosso laboratório de pesquisas (LRM – ICMC – USP) é completamente proibido experimentos com veículos em modo autônomo sem uma pessoa DENTRO do veículo.

### Referente a Robótica:

Um robô não pode JAMAIS decidir sobre a vida ou morte de uma pessoa. O Brasil deve ratificar as moções da ONU e de diferentes organismos internacionais sobre “robôs que matam”. Mesmo robôs militares não PODEM de modo algum decidir sozinhos se vão matar pessoas. Qualquer decisão, mesmo em situação de guerra, tem que ter um responsável pela decisão e ação, que poderá depois ser julgado pelas suas decisões, ações e ordens dadas.

- Este movimento é conhecido como: “*Stop Killer Robots*” ( <https://www.stopkillerrobots.org/> )
- Referências adicionais:
  - <https://www.hrw.org/topic/arms/killer-robots> Human Rights Watch
  - [https://en.wikipedia.org/wiki/Campaign\\_to\\_Stop\\_Killer\\_Robots](https://en.wikipedia.org/wiki/Campaign_to_Stop_Killer_Robots)
  - <https://www.reuters.com/world/un-chief-urges-action-killer-robots-geneva-talks-open-2021-12-13/>
  - <https://www.stopkillerrobots.org/news/unban/>

Uma máquina não pode ter o poder de decisão sobre a vida e a morte de uma pessoa. Nunca!

(\*) Mesmo os “drones” militares dos USA são controlados remotamente, e a decisão de atacar é humana.

## Referente a Sistemas Inteligentes:

1. Todo sistema inteligente que utilize aprendizado de máquina (*machine learning*) deve ser transparente e auditável, ou seja, devem ser “armazenados” todos os dados e programas usados para colocar um determinado sistema de Inteligência Artificial, baseado em aprendizado, em produção. Em caso de processos, danos, e da necessidade de uma auditoria externa, deve ser possível para os órgãos responsáveis pela investigação (a serem definidos em legislação própria para tal), que tenham acesso a estes dados.

Por exemplo, um sistema de diagnóstico médico baseado em Inteligência Artificial tem que ter os dados de treinamento (*datasets* e bases de aprendizado: dados “congelados” nas diferentes versões disponibilizadas para uso), armazenados e disponibilizados em caso de necessidade de uma auditoria e investigação sobre erros, falhas e danos causados pelo uso do sistema. Além dos dados, também é necessário que uma cópia do sistema seja armazenada e disponibilizada em caso de investigação (incluindo, por exemplo, redes de *deep learning* treinadas e usadas pelo sistema).

O objetivo desta “guarda de dados de treino e de sistemas” é poder avaliar o BIAS (tendências e desvios de comportamento) dos sistemas que possam ser prejudiciais aos usuários, com a identificação se existe alguma responsabilidade dos proprietários do sistema, pelo treino inadequado e pelas respostas do mesmo, que possam vir a causar danos a terceiros.

Os dados e programas que seriam auditáveis permanecem sigilosos, sendo apenas acessados pelos responsáveis da investigação, e que devem garantir que não haja vazamentos de dados.

Essa proposta visa criar sistemas AUDITÁVEIS, de modo a poder responsabilizar adequadamente aqueles que tenham alguma culpa/responsabilidade pelos danos causados pelos sistemas de I.A. Podemos fazer uma analogia com produtos farmacêuticos, onde a fórmula do remédio (composição) deve ser registrada, neste caso, a composição do sistema é composta pelos programas E TAMBÉM pelos dados usados para treinar a I.A. do sistema.

## Referente a Privacidade e o Respeito ao Indivíduo:

Acredito que devemos seguir o exemplo da LGPD (e a GDPR) no que diz respeito ao armazenamento e acesso a dados pessoais. Já existe uma legislação mais geral a esse respeito.

## Referente a Propriedade Intelectual:

Máquinas não são conscientes. Máquinas podem gerar informações de modo totalmente espontâneo e criativo. Máquinas geram “saídas” apenas quando uma pessoa fornece os dados de entrada e estimula o sistema a gerar um produto de saída. No meu entender, máquinas NÃO são proprietárias de obras literárias, musicais, ou, de arte (ou até mesmo patentes). O proprietário continua sendo o programador, ou, aquele que configura o sistema, ou, quem executa o sistema que leva a geração de uma obra: esse é o responsável, o proprietário, e quem deve responder legalmente pela obra criada (inclusive pode responder por plágios criados pela máquina). Tem que ter um responsável pelo produto final.

Assim como no caso dos robôs assassinos, ou, no caso das máquinas criativas, sempre deve haver uma pessoa responsável pela ação, pela criação, e que pode inclusive ser responsabilizada e processada pelos danos que venham a ser causados pela “sua máquina ou pelos atos da máquina”.

Agradeço a atenção dispensada, e espero ter contribuído para uma melhor regulamentação da I.A.,  
Prof. Dr. Fernando Santos Osório.