ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

PREVISÃO DE PENAS DE MULTA DE CRIMES CIBERNÉTICOS NO BRASIL: UMA CONTRIBUIÇÃO DO APRENDIZADO DE MÁQUINA E DA INTELIGÊNCIA ARTIFICIAL EXPLICÁVEL.

Cibele Andréa de Godoy Fonseca[1]

Ismar Frango Silveira[2]

Marco Vallim[3]

RESUMO

Este artigo apresenta o uso da 'inteligência artificial explicável' no contexto da previsão de penas de multa de crimes cibernéticos e para atingir esse objetivo primeiro é conduzida a previsão de penas de multa aplicadas pelos tribunais brasileiros referentes aos crimes cibernéticos utilizando dados coletados dos processos de coisa julgada e do aprendizado de máquina, e em seguida é feita a explicação de quais fatores, dentre os presentes no modelo, que mais influenciam os resultados da previsão. Essa previsão será feita obedecendo às fases da metodologia de descoberta de conhecimento em banco de dados (*KDD*) e com o uso de dois algoritmos de aprendizado de máquina supervisionado. Os resultados tendem a ajudar especialistas a descobrir os fatores que podem influenciar nos padrões de aplicação de penas de multa pelos tribunais e com base nesses padrões fazer análises e previsões.

Palavras-chave: Aprendizado de máquina; CBA; Crimes cibernéticos; Inteligência artificial explicável; XGBoost.

ABSTRACT

This article presents the use of 'explainable artificial intelligence' in the context of forecasting fines for cybercrimes and to achieve this objective, first a forecast of fines imposed by Brazilian courts regarding cybercrimes is conducted using data collected from res judicata and machine learning, and then the explanation of which factors, among those present in the model, that most influence the prediction results is made. This prediction will be made according to the phases

[1] Advogada, Bacharel em Ciências com Licenciatura em Matemática, Doutora e Mestre em Engenharia Elétrica e Computação. Profissional com mais de 20 anos de experiência em cargos executivos responsável pela Área de Tecnologia da informação. lattes.cnpq.br/0780179952438526.

[2] Graduado em Matemática, Mestre em Ciências e Doutor em Engenharia Elétrica. Professor Adjunto da Universidade Presbiteriana Mackenzie e Professor Titular da Universidade Cruzeiro do Sul. Membro das comunidades científicas LA CLO (Comunidade Latino-Americana de Tecnologias de Aprendizagem), HCI-Collab (Rede Colaborativa para apoiar os processos de ensino e aprendizagem em área de Interação Humano-Computador em nível Iberoamericano), e VG-Collab (Rede Colaborativa de pesquisa e desenvolvimento de jogos na Iberoamérica). http://lattes.cnpq.br/3894359521286830.

[3] Mestre e Doutorando em Engenharia Elétrica e Computação com ênfase em Ciência de Dados, Bacharel em Sistemas de Informação, Especialista em Finanças Empresariais e Bacharel em Ciências Econômicas pela Universidade Presbiteriana Mackenzie. http://lattes.cnpq.br/0597940054574281.

of the database knowledge discovery methodology (KDD) and with the use of two supervised machine learning algorithms. The results tend to help specialists to discover the factors that may influence the patterns of application of fines by the courts and, based on these patterns, to make analyzes and predictions.

Keywords: Machine learning; CBA; Cybercrimes; Explainable artificial intelligence; XGBoost.

1 INTRODUÇÃO

Saúde, privacidade e visão computacional são algumas das áreas em que a inteligência artificial tem espaço consolidado. Sua aplicação tem se expandido também de forma consistente no Direito. Note-se que a inteligência artificial nos assuntos do Judiciário vem sendo adotada pelo Brasil e este tema está incluído no projeto intitulado de Justiça 4.0 CNJ, do Conselho Nacional de Justiça (2022).

Chama a atenção, nesse sentido, a temática e a aplicação potencial aos crimes cibernéticos. No Brasil, esse tipo de delito tem crescido, algo verificado sobretudo nos anos de 2020 e 2021, em função do isolamento causado pela pandemia de Covid-19. Conforme KHOUALED et al. (2022), as condições de quarentena e o distanciamento social também tiveram um impacto significativo no crescimento desenfreado de usuários digitais em todo o mundo, que totalizaram 7,38 bilhões de pessoas, um aumento de 56,4% em relação a 2019, com 5,22 bilhões usando smartphones e 4,66 bilhões usando a internet.

Este novo contexto permitiu a criminosos usarem os meios digitais e cometerem crimes e delitos, inclusive no Brasil. O país ficou em 2º lugar no número de ataques na América Latina e Caribe, atrás apenas do México (156 bilhões) e à frente do Peru (11,5 bilhões) e da Colômbia (11,2 bilhões). O aumento foi constante ao longo do ano e observado em toda a região. Ao todo, houve 289 bilhões de ataques, 600% a mais em comparação ao ano anterior (41 bilhões)[4]. De acordo com Steve Morgan, o cibercrime custará ao mundo 8 trilhões em 2023 e ele ainda ressalta que, caso ele fosse medido como um país, seria equivalente à terceira maior economia do mundo, depois apenas de China e de Estados Unidos, conforme MORGAN, Steve (2022).

[4] SECURITY REPORT. Disponível em: https://www.securityreport.com.br/overview/brasil-sofreu-mais-de-885-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2021/. Acesso em: 28 set. 2022.

Cabe aqui trazer a abordagem de Nivette et. All (2021), segundo os quais as motivações para cometer crimes cibernéticos estão conectadas às restrições aos movimentos populacionais oriundas de epidemias, de desastres naturais ou de apagões uma vez que durante esses movimentos o uso de tecnologias aumenta. Os autores explicam, ainda, que os níveis de estresse e emoções negativas, tais como ansiedade, frustração e raiva são motivadas pelas restrições citadas.

A partir desse contexto, a proposta é abordar o uso da 'inteligência artificial explicável' (em inglês - *explainable artificial intelligence*, ou XAI), a qual tem sido utilizada para apresentar quais fatores afetam os resultados dos modelos de aprendizado de máquina. A justificativa para o uso da XAI se refere à necessidade de se evitar vieses quanto ao uso da inteligência artificial. De acordo com SATYA, *et al,* (2022), "XAI tenta fornecer mais informações sobre os modelos de caixa preta e suas interações internas que permitem aos humanos entender uma saída gerada por máquina".

Os já citados percentuais de crimes cibernéticos ocorridos recentemente no Brasil, as tendências da sua ocorrência no mundo e seus impactos financeiros, no contexto da XAI, podem contribuir para a previsão das decisões tomadas pelos tribunais brasileiros, quando elas visam apenar os crimes cibernéticos por meio da aplicação de multa. Trata-se de um trabalho interdisciplinar, que contribui para a mais justa e efetiva aplicação da lei penal no país.

2 PADRÕES DE APLICAÇÃO DE MULTA

Este trabalho, que une tecnologia e direito, discute como principal problema a produção de resultados para ajudar especialistas a descobrirem padrões de aplicação de multas pelos tribunais em face de um conjunto de leis aplicadas. A proposta é obter de forma eficaz previsões, por meio dos dados coletados dos processos que já têm coisa julgada, a partir do uso do aprendizado de máquina.

Inicialmente, é importante contextualizar o que já é feito para se realizar previsões acerca dos crimes cibernéticos com o uso de inteligência artificial e dados de crimes. O trabalho aqui proposto, pois, inova na medida em que utiliza dados oriundos dos processos de coisa julgada, e não de relatórios criminais ou de pesquisas feitas com os cidadãos.

Segundo Greenstein (2022), a inteligência artificial está sendo cada vez mais incorporada a sistemas destinados a auxiliar os atores do sistema de justiça criminal em suas tomadas de decisão e responsabilidades. Um desses exemplos é o uso de sistemas que incorporam modelos para auxiliar juízes na tomada de decisões sobre pessoas em várias circunstâncias: por exemplo, se uma pessoa deve ser libertada julgamento pendente. Até mesmo para definir a severidade de uma sentença.

No presente estudo, foram pesquisados trabalhos que utilizaram dados heterogêneos com aprendizagem de máquina para analisar e prever crimes. U. Rosa Monteiro de Castro (2020) contemplou em seu trabalho o uso de cinco técnicas de aprendizado de máquina: k-NN, SVM, Random Forest, XGBoost e LSTM. Os dados utilizados são provenientes de fontes heterogêneas, contêm registros criminais oficiais e não oficiais e incluem um conjunto de antecedentes criminais oficiais coletados junto à Secretaria de Segurança do Estado de Minas de Gerais (Brasil) e um conjunto de dados não oficiais coletados do site do projeto independente 'Onde foi roubado'.

Por sua vez, J. Renato Mendes Souza (2018) utiliza em seu trabalho os algoritmos 'Árvore de Decisão', 'Classificação Gaussiana Naive Bayes' e 'K-NN K-Nearest Neighbor', além de dados criminais fornecidos pelo site 'Dados Abertos do Instituto de Segurança Pública do Estado do Rio de Janeiro' pelo qual é possível acessar as bases de dados de antecedentes criminais e a atividade policial no estado do Rio de Janeiro.

S.Wang (2017) usou os algoritmos K-means e K-Nearest Neighbors, além de um conjunto de dados relativos a taxas de crimes de ódio praticados nos EUA em 2016, antes e depois da eleição presidencial, e de todos os estados dos EUA, de 2010 a 2015. W. Safat, Wajiha, S. Asghar y S. Andleeb Gillani (2021) usaram dados criminais de Chicago e de Los Angeles (EUA) e os algoritmos Logistic Regression, SVM, Naïve Bayes, KNN, Decision Tree, MLP, Random Forest, XGBoost e LSTM.

A. Stec e D. Klabjan (2018) utilizaram redes neurais profundas para prever a contagem de crimes no dia seguinte de suas ocorrências. Integram o *dataset* os dados de crimes de Chicago e Portland (EUA), somadas às informações referentes ao clima, ao censo e ao transporte público. Y. Rayhan e T. Hashem (2021), por sua vez, utilizaram nesse trabalho os dados referentes aos crimes ocorridos em Chicago (EUA) e o *deep learning* para conduzir seus estudos baseados em dados históricos.

S. Sappa Kshatri, *et al*. (2021), por meio do aprendizado de máquina e do comitê de máquinas, pesquisaram a previsão de crimes na Índia, país desafiador no que diz respeito à identificação da natureza dinâmica dos crimes.

O *dataset* foi elaborado com base nos dados criminais de 2001 a 2015, oriundos dos registros de crimes do National Crime Record Bureau (NCRB) de todos os estados da Índia referentes aos relatórios factuais sobre assassinato, estupro e roubo (crimes violentos). Cerca de 60.000 crimes ocorreram nesse período (KSHATRI, 2021).

Baseado nos resultados da contextualização é possível afirmar que, nos casos apresentados, não foram utilizados:

(i) dados coletados dos processos de coisa julgada e aprendizado de máquina para fazer análises e previsões; e

(ii) não foi utilizado o algoritmo CBA (Classificação Baseada em Mineração de Regras de Associação), para explicar quais fatores, dentre os presentes no modelo, que mais influenciam os resultados da previsão.

Devido a essas afirmações, é possível destacar o ineditismo da metodologia e resultados deste artigo.

3 SOLUÇÃO PROPOSTA

Nesta seção, evidencia-se a interdisciplinariedade da pesquisa. Será pormenorizada a base tecnológica que permite a obtenção dos dados.

3.1 Tecnologias

Integram a solução proposta o uso da Metodologia KDD (em inglês, *knowledge discovery in database*, ou descoberta de conhecimento em base de dados), bem como os modelos de classificação XGBoost e CBA.

As avaliações do resultado do modelo com XGBoost são realizadas com base nas métricas de acuracidade, *precision*, *recall*, da matriz de confusão e da curva ROC.

Ao final, serão explicados os atributos que mais impactaram o modelo por meio do uso do CBA e da avaliação da sua acurácia, bem como dos seus índices de suporte e confiança para cada regra destacada.

Vale ressaltar que o algoritmo XGboost foi escolhido por ser a versão mais avançada entre os modelos de aprendizado de máquina. Ele consome menor capacidade de máquina se comparado aos outros modelos de classificação e apresenta, ainda, maior convergência.

O CBA por sua vez, foi escolhido para representar a XAI. Proposto por Liu et al. (1998), ele consiste em duas partes, que integram as tarefas de extração e descoberta. O gerador de regras, que utiliza uma abordagem Apriori (algoritmo) para descobrir as regras de classificação, é baseado em relacionamentos frequentes encontrados na base de dados.

Este subconjunto de regras é chamado de *class association rules* (CARs) (LIU et al., 1998; AGRAWAL; SRIKANT et al., 1994). Chamado por Liu et al. (1998) de CBA-RG, o algoritmo gera todas as chamadas *ruleitems*, enquanto passa diversas vezes pelo conjunto de dados. Inicialmente, ele determina o suporte individual de cada regra e aponta quais são as frequentes. Nas interações seguintes, apenas analisa aqueles que foram considerados frequentes de acordo com a interação anterior.

3.2 Modelo baseado nas fases da KDD

Nesta seção, composta de tabelas que trazem os resultados da pesquisa realizada pelos autores, apresenta-se o uso da tecnologia Python com as suas bibliotecas acessórias e as fases da metodologia KDD. Note-se que já se contempla a definição do problema a ser resolvido.

Seleção de dados: nesta fase, foi estruturado um *dataset* intitulado ‘resjudicata’, no formato CSV (do inglês *comma-separated values*) contendo 7.274 registros.

Esses dados foram extraídos da plataforma Juit 2, em 29/6/2022, referentes aos processos com coisa julgada (*res judicata*) dos crimes cibernéticos ocorridos entre janeiro de 2006 e junho 2022. A Tabela 1 traz o dicionário de dados desse *dataset*.

Quadro 1: Dicionário de dados do *dataset* Resjudicata

Nome	Descrição	Tipo	Tamanho
process_id	número do processo	continuous numeric	5
court	local do julgamento	continuous numeric	14
data_publish	data da publicação	continuous numeric	10
cnj_theme_name_list	área do direito	nominal categorical	207
cite_legislation_list	lei para aplicação da pena	nominal categorical	255
max_value	valor da pena	continuous numeric	15
max_value_currency	tipo de moeda	nominal categorical	10

Fonte: produzido pelos autores.

Pré-processamento e limpeza de dados: nesta fase, foram conhecidos os atributos. Houve limpeza e padronização de strings, por meio da remoção de informações, limpeza de espaços vazios, correção de caracteres e a desambiguação de informações.

Transformação de dados: nesta fase, foram conduzidas as seguintes atividades:

1) Transformação dos conteúdos dos atributos ‘cnj_theme_name_list’ e ‘cite_legislation_list’ em colunas. Os atributos do conjunto de dados Resjudicata permaneceram de acordo com a Tabela 1;

2) Após a condução da atividade 1, identificou-se que algumas áreas do Direito brasileiro não estavam expressas conforme são publicadas pelo Conselho Nacional de Justiça (CNJ). Essa descoberta levou à execução de um *script* em Python para normalizar a situação. O resultado foi um *dataset* intitulado ‘resjudicata1’, com 139.991 registros. O número foi mantido, pois os dados por ‘process_id’ nos atributos ‘cite_legislation_list’ e ‘cnj_theme_name_list’ foram lidos e cada área do Direito encontrada no ‘cnj_theme_name_list’ foi transformada em um registro. Além disso, as leis encontradas no atributo ‘cite_legislation_list’ também foram transformadas em um registro.

O resultado da análise exploratória dos dados do ‘resjudicata1’ é apresentada na Tabela 2. Elas demonstram as quantidades de áreas do Direito contempladas nos processos com coisa julgada utilizados pelos tribunais em seus julgamentos. Vale destacar que foram considerados tribunais federais e estaduais, bem como tribunais superiores, num amplo espectro de análise.

Quadro 2: Quantidade de áreas do Direito por Tribunal

Tribunal	Descrição	Quantidade
STJ	Superior Tribunal de Justiça	19
TJSP	Tribunal de Justiça de São Paulo	19
STF	Superior Tribunal Federal	18
TJMS	Tribunal de Justiça do Mato Grosso do Sul	15
TJAL	Tribunal de Justiça do Estado de Alagoas	14
TRF3	Tribunal Regional Federal da 3ª Região	13
TJCE	Tribunal de Justiça do Estado do Ceará	12
TRF1	Tribunal Regional Federal da 1ª Região	11
TRF4	Tribunal Regional Federal da 4ª Região	10
TRF5	Tribunal Regional Federal da 5ª Região	10
TJRS	Tribunal de Justiça do Estado do Rio Grande do Sul	9
TJDFT	Tribunal de Justiça do Distrito Federal e dos Territórios	7
TRF2	Tribunal Regional Federal da 2ª Região	7
TJAM	Tribunal de Justiça do Amazonas	6
TST	Tribunal Superior do Trabalho	6

Fonte: produzido pelos autores.

Conforme se observa, os tribunais STJ (tribunal superior que se dedica à legislação ordinária), TJSP (o maior tribunal da justiça comum estadual do país) e STF (a corte suprema do país, que se ocupa da Constituição Federal) são os que utilizam a maior quantidade de áreas do Direito em seus julgamentos, em razão de julgarem crimes cibernéticos mais complexos. Portanto, há uma amplitude de temas que se interconectam nas análises.

3) Classificação de penalidades: para prever penas de multa foi necessário classificar as penalidades a partir da criação do *dataset* Lawarticle, que contém os atributos apresentados no dicionário de dados trazidos na Tabela 3. Após criar o *dataset*, os pesquisadores verificaram cada lei utilizada pelos tribunais. Foram incluídas as penas que são classificadas em ‘restritiva de liberdade’, ‘restritiva de direito’ e ‘multa’.

Quadro 3: Atributos do *dataset* LawArticle

Nome	Descrição	Tipo	Tamanho
cite_legislation_list	lei para aplicação da pena	nominal categorical	255
restrictive_of_liberty	pena restritiva de liberdade	continuous numeric	1
restrictive_of_right	pena restritiva de direito	continuous numeric	1
reclusion	pena de reclusão	continuous numeric	1
detention	pena de detenção	continuous numeric	1
pecuniary_fine	multa	continuous numeric	1

Fonte: produzido pelos autores.

4) Após classificar as penalidades, os *datasets* 'resjudicata1' e 'LawArticle' foram unidos com a execução do comando join do Python, por meio do atributo 'process_id'. O resultado foi o *dataset* 'resjudicata1' composto de 19.172 registros, cujos atributos constam da Tabela 4.

Quadro 4: Atributos do *dataset* Resjudicata1

Nome	Descrição	Tipo	Tamanho
process_id	número do processo	continuous numeric	5
court	local do julgamento	continuous numeric	14
data_publish	data da publicação	continuous numeric	10
cnj_theme_name_list	área do direito	nominal categorical	207
cite_legislation_list	lei para aplicação da pena	nominal categorical	255
max_value	valor da pena	continuous numeric	15
max_value_currency	tipo de moeda	nominal categorical	10
restrictive_of_liberty	pena restritiva de liberdade	continuous numeric	1
restrictive_of_right	pena restritiva de direito	continuous numeric	1
reclusion	pena de reclusão	continuous numeric	1
detention	pena de detenção	continuous numeric	1
pecuniary_fine	Multa	continuous numeric	1

Fonte: produzido pelos autores.

A partir da utilização da análise exploratória de dados, a Tabela 5 mostra o número de leis usadas pelos tribunais para apenar crimes cibernéticos.

Quadro 5: Quantidade de leis por tribunal

Tribunal	Quantidade
TJSP	1.441
STJ	1.154
TST	337
STF	209
TRF3	198
TRF5	87
TRF1	76
TJMS	48
TRF4	25
TJCE	21
TJAL	17
TRF2	12
TJDFT	8
TJAM	7
TJRS	6

Fonte: produzido pelos autores.

Como resumo da análise exploratória, afirma-se que os tribunais TJSP, STJ e TST são os que utilizam maior quantidade de leis, se comparados aos outros tribunais. Logo, são os que julgam crimes cibernéticos de maior complexidade.

A Tabela 6 apresenta as quantidades por tipo de penalidade utilizada pelos tribunais em seus julgamentos. A análise revela que os tribunais do STJ e do TJSP são os que mais apenam os crimes cibernéticos com multa.

Quadro 6: Quantidade de penalidades por tribunal

Tribunal	Restritiva de liberdade	Restritiva de direito	Multa
STF	45	41	79
STJ	1.033	948	1.618
TJAL	1	1	3
TJAM	0	0	2
TJCE	1	2	7
TJDFT	3	2	4
TJMS	16	14	52
TJRS	5	6	7
TJSP	822	1.451	2.726
TRF1	35	29	46
TRF2	0	0	3
TRF3	195	177	230
TRF4	17	19	22
TRF5	77	66	83
TST	24	402	1.225

Fonte: produzido pelos autores.

Na Tabela 7, apresenta-se a quantidade de penas de reclusão e de detenção aplicadas por tribunal.

Quadro 7: Quantidade de penas de reclusão e de detenção por tribunal

Tribunal	Reclusão	Detenção
STF	41	38
STJ	960	960
TJAL	1	1
TJAM	0	0
TJCE	1	1
TJDFT	3	3

TJMS	15	13
TJRS	5	5
TJSP	447	752
TRF1	35	29
TRF2	0	0
TRF3	187	191
TRF4	17	15
TRF5	75	62
TST	15	21

Fonte: produzido pelos autores.

Analisando a distribuição da reclusão e da detenção, verifica-se que o STJ seguido do TJSP são os tribunais que mais aplicam essas penalidades. O terceiro é o TRF3 (tribunal federal responsável pela tramitação de ações nos Estados de São Paulo e Mato Grosso do Sul). Na fase de mineração de dados (fase da KDD), foi executado o algoritmo XGBoost.

Quadro 8: Matriz de confusão

	Pena de multa	Não pena de multa
Pena de multa	4.304	19
Não pena de multa	168	1.836

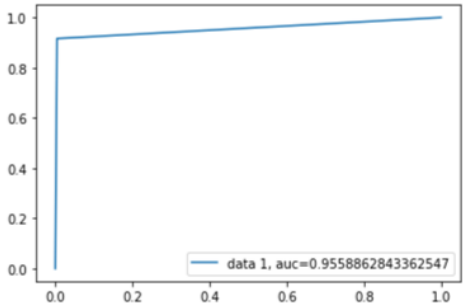
Fonte: produzido pelos autores.

Quadro 9: *Precision*(%), *recall*(%), *f1-score*(%) e *support* (quantidade)

	precision	*recall*	*f1-score*	*support*
False	0.96	1.00	0.98	4.323
True	0.99	0.92	0.95	2.004
Accuracy			0.97	6.327
Macro avg	0.98	0.96	0.97	6.327
Weighted avg	0.97	0.96	0.97	6.327

Fonte: produzido pelos autores.

Figura 1: Curva ROC



Fonte: produzido pelos autores.

4 INTERPRETAÇÃO E AVALIAÇÃO DOS RESULTADOS

4.1 Avaliação dos resultados do Algoritmo XGBoost

É possível dizer que as estatísticas coletadas consistem em um indicador de acuracidade global de 97,04%, indicando que o modelo atingiu um bom valor, sem a necessidade de se alterar parâmetros. Isso significa dizer que, para cada 100 casos, **o modelo foi capaz de prever corretamente 97,04 vezes se a pena aplicada contempla multa pecuniária**.

O próximo passo consiste em analisar as estatísticas *precision* e *recall*, para observar o *trade-off* entre viés e variância. Isso demonstra precisamente o que está ocorrendo com o modelo no processo de tomada de decisão.

De acordo com a Tabela 9, as médias ponderadas revelam 97% de *precision* e 96% de *recall*, indicando um modelo bastante confiável em relação ao balanceamento entre os verdadeiros positivos e os verdadeiros negativos. Mitiga-se a probabilidade de se cometer os erros tipo 1 e os erros tipo 2 (tipo 1: aceitar a hipótese nula quando ela é falsa; tipo 2: rejeitá-la quando é verdadeira).

A qualidade do modelo também pode ser validada observando a matriz de confusão. Neste caso, tanto os verdadeiros positivos quanto os verdadeiros falsos estão aderentes. Observam-se poucas situações de falsos positivos e falsos negativos, o que demonstra que o modelo está generalizando de forma eficaz.

Por fim, é possível validar a curva ROC do modelo apresentada na figura 5, cuja estatística está em 95%, aderente com o encontrado até aqui. Ela mostra que o ponto de interseção entre o FPR e o TPR é 0,9, próximo de 1. Tal dado revela uma alta taxa de precisão.

Ao analisar os resultados das métricas de *precision*, *recall*, *f1-score* e *support* apresentadas na Tabela 9, ressalta-se: quanto à *precision*, 96% das multas não pecuniárias encontradas são corretas e 99% das multas pecuniárias são incorretas. No caso da *recall*, o modelo identificou 100% dos falsos. Isso significa 100% do valor de multas não pecuniárias e 92% de multas pecuniárias.

Quanto à *f1-score*, 97% é um percentual alto como média harmônica entre *precision* e *recall*. Com relação ao *support*, foram encontradas 4.323 multas não pecuniárias e 2.004 multas pecuniárias. Todas as métricas estão acima de 90%, o que leva à conclusão de que o modelo traz uma boa resposta com base nos dados usados para testes e treino.

4.2 Avaliação de resultados do XGBoost com CBA

Os atributos ‘court’, ‘cite_legislation_list’, ‘max_value’, ‘restrictive_of_right’ e’ pecuniary_fine’ foram selecionados para a execução do modelo com o algoritmo CBA. As variáveis *default* do algoritmo foram assim definidas de acordo com a Tabela 10:

Quadro 10: S*upport* (quantidade) e *Confidence* (percentual)

Support	*Confidence*
0.02	0.60

Fonte: produzido pelos autores.

Os primeiros testes apresentaram baixos índices de suporte para a maioria das regras descobertas pelo modelo (o maior índice de suporte observado foi de 0.17%). Isso ocorre devido ao fato de existirem diversas combinações possíveis em uma base relativamente grande e complexa, lastreada na realidade, mesmo após o pré-processamento. Para fins de evitar explosão de regras e, mesmo assim, não podar regras relevantes com alto índice de confiança, o suporte mínimo determinado foi de 0.02%. Quanto à confiança mínima, ela foi definida com

0.60%, contudo, ao observar os resultados, ficou claro que esse valor pouco influenciou, já que todas as regras apresentaram confiança igual ou superior a 0.99%.

As regras extraídas do modelo treinado com 75% dos dados utilizados na modelagem do XGBoost podem ser observadas na figura 2.

Figura 2: Regras do CBA

```
[CAR {cite_legislation_list=L11419} => {pecuniary_fine=0.0} sup: 0.03 conf: 1.00 len: 2, id: 9,
 CAR {cite_legislation_list=L13105} => {pecuniary_fine=0.0} sup: 0.02 conf: 1.00 len: 2, id: 5,
 CAR {cite_legislation_list=L16} => {pecuniary_fine=0.0} sup: 0.02 conf: 1.00 len: 2, id: 3,
 CAR {cite_legislation_list=L01} => {pecuniary_fine=0.0} sup: 0.02 conf: 1.00 len: 2, id: 1,
 CAR {restrictive_of_right=1,court=TST} => {pecuniary_fine=1.0} sup: 0.02 conf: 0.99 len: 3, id: 10,
 CAR {restrictive_of_right=1,court=TJSP} => {pecuniary_fine=1.0} sup: 0.08 conf: 0.99 len: 3, id: 13,
 CAR {restrictive_of_right=1} => {pecuniary_fine=1.0} sup: 0.17 conf: 0.99 len: 2, id: 14]
```

Fonte: produzido pelos autores.

É possível observar muitas regras relacionadas à ocorrência de pena de multa com a pena restritiva de direito. Isso se deve ao fato de que a ocorrência de multa, muitas vezes, está relacionada à complexidade do crime e à gravidade dos fatos nele envolvidos. Também pode-se observar que sentenças com penas restritivas de direito nos tribunais TST e TJSP tendem a incluir multa pecuniária.

5 CONSIDERAÇÕES FINAIS

A partir da análise exploratória dos dados e seguindo as fases da metodologia KDD, conclui-se que os tribunais TJSP, STJ e TST (corte superior dedicada a ações trabalhistas) são os que utilizam maior quantidade de leis quando comparados aos outros tribunais. Portanto, são os que julgam crimes cibernéticos de maior complexidade.

Ainda, os tribunais STJ, TJSP e STF são os que utilizam a maior quantidade de áreas do direito em seus julgamentos, o que ocorre porque julgam crimes cibernéticos mais complexos. As outras conclusões referem-se às penas de reclusão e de detenção. Nesse contexto, verifica-se que o STJ e o TJSP são os tribunais que mais aplicam essas penalidades, seguidos pelo TRF3. Já o STJ e o TJSP são os que mais aplicam a pena de multa. Aqui, cabe anotar o volume de processos e o contexto socioeconômico do Estado de São Paulo, que detém o maior PIB do país. Abrem-se possibilidades de futuras pesquisas centradas nas relações entre TRF3, TJSP e os tribunais superiores, especificamente.

Quanto à execução do XGBoost, é possível observar que o modelo apresenta métricas de valores altos. Portanto, os dados utilizados possuem grande convergência. Em relação às métricas do CBA, é possível afirmar que os seus resultados são coerentes tanto com o resultado apresentado pelo XGBoost quanto pelas decisões dos tribunais.

A alta acurácia do classificador corrobora a grande convergência do XGBoost e as regras que foram geradas pelo modelo possuem forte lastro no sistema jurídico. Nota-se que o atributo 'cite_legislation_list' está presente nas regras com maior índice de suporte, indicando que, para casos menos complexos, em que se evoca apenas uma lei (e ela estando em uma das regras geradas), a tendência é o crime não ser apenado com pena de multa pecuniária.

Casos mais complexos, cujas penas culminam em restritivas de direito, costumam vir acompanhadas de multa pecuniária e isso se deve ao fato da complexidade do crime. Os tribunais TST e TJSP foram os que mais apenaram crimes dessa natureza.

Conforme as métricas apresentadas, verifica-se que os dados dos processos 'resjudicata' e aprendizado de máquina podem ser usados para conduzir outras análises e previsões referentes aos crimes cibernéticos. Assim, os resultados deste experimento se mostram promissores para a análise de dados jurídicos, em especial em relação aos atributos escolhidos como *proxies* das disciplinas (as grandes áreas do direito, e estas estão relacionadas às leis, que são partes menores das disciplinas). Por sua vez, determinam de acordo com o tipo de crime cometido o que acontece com o réu após o tribunal proferir a sentença.

Em uma futura ampliação do trabalho, novos atributos podem ser escolhidos, ampliando o seu escopo rumo à jurimetria, disciplina que tem se tornado protagonista nas áreas de intersecção entre Direito, estatística e ciência de dados em geral. Outras propostas incluem o uso de um algoritmo de classificação e previsão com o conjunto de dados de coisa julgada conforme especificado abaixo:

1. Realizar a previsão das penas restritiva de liberdade e restritiva de direitos;

2. Realizar a previsão de em sendo penas restritiva de liberdade, se a decisão foi de pena de reclusão ou de detenção;

3. Implementar o CBA como metodologia de *boosting* para o XGBoost, visando compreender e incrementar as suas predições, buscando classificar os (poucos) registros em que o XGBoost erra;

4. Elaborar relatórios contendo os resultados dos modelos para que os especialistas possam adequar as suas propostas dentro dos seus escopos de trabalho. É possivel citar o caso de um(a) advogado(a) que ao entender a decisão de determinado tribunal, poderá antecipar-se quanto às suas teorias de defesa.

Como proposta, baseado nas considerações de Cynthia Rudin (2019), destaca-se a importância da utilização de modelos interpretáveis nos trabalhos futuros no lugar da utilização de modelos de aprendizado de máquina que mostrem os atributos que mais impactaram nos resultados do modelo.

REFERÊNCIAS

CASTRO, Ursula Rosa Monteiro de. **Explorando aprendizagem supervisionada em dados heterogêneos para predição de crimes**. Dissertação (Mestrado em Informática). Pontifícia Universidade Católica de Minas Gerais (PUC-MG), Minas Gerais, 2020.

AGRAWAL, Rakesh; SRIKANT, Ramakrishnan. **Fast algorithms for mining association rules**. Proc. of 20th Intl. Conf. on VLDB, 1994.

AL-MAOLEGI, M.; ARKOK, B. Na, improved apriori algorith for association rules. **International Journal on Natural Language Computing (IJNLC)**, Computer Science, Jordan University of Science and Technology, Irbid, Jordan, 2014.

CNJ. **Justiça 4.0: Inteligência Artificial está presente na maioria dos tribunais brasileiros**. Disponível em: https://www.cnj.jus.br/justica-4-0-inteligencia-artificial-esta-presente-na-maioria-dos-tribunais-brasileiros/. Acesso em: 22 dez. 2022.

GREENSTEIN, S. Preserving the rule of law in the era of artificial intelligence (AI). Artif Intell Law 30, 291–323 (2022). Disponível em: https://doi.org/10.1007/s10506-021-09294-4. Acesso em: 26 set. 2022.

INSTITUTO DE SEGURANÇA PÚBLICA. **Dados abertos**. Governo do Estado do Rio de Janeiro. Disponível em: http://www.ispdados.rj.gov.br/. Acesso em: 26 set. 2022.
ISSN 0031-3203, https://doi.org/10.1016/j.patcog.2022.108604.

KHOUALED et al. "Corona Pandemic (Covid-19) and Information and Communication Technology (ICT): Who Affects Whom?". Revista Geintec – Gestão, Inovação e Tecnologia. Vol. 12, n. 1, ISSN 2237-0722. P. 132-147. Disponível em: https://revistageintec.net/wp-content/uploads/2022/12/02_9066_Revista-geintec-gestao-inovacao-e-tecnologias.pdf. Acesso em: 26 set. 2022.

KSHATRI, S. Sappa; *et al.* An empirical analysis of machine learning algorithms for crime prediction using stacked generalization: An ensemble approach. **IEEE Access** v. 9, p. 67488-67500, 2021.

MORGAN, Steve. Cybercrime To Cost The World 8 Trillion Annually In 2023. Disponível em: https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/. Acesso em: 23 dez. 2022.

NIVETTE, A.E., Zahnow, R., Aguilar, R. *et al.* A global analysis of the impact of COVID-19 stay-at-home restrictions on crime. *Nat Hum Behav* **5**, 868–877 (2021). Disponível em: https://www.nature.com/articles/s41562-021-01139-z. Acesso em: 26 set. 2022.

OLIVEIRA, Ingrid. Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%. **CNN Brasil**. 19 ago. 2022. Disponível em: https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/. Acesso em: 26 set. 2022.

RAYHAN, Y.; HASHEM, T. **AIST**: An interpretable attention-based deep learning model for crime prediction. https://doi.org/10.48550/arXiv.2012.08713. Revisado em 21 nov. 2021. Disponível em: https://arxiv.org/abs/2012.08713. Acesso em: 26 set. 2022.

RUDIN, C. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nat Mach Intell 1, 206–215 (2019). Disponível em: https://doi.org/10.1038/s42256-019-0048-x. Acesso em: 26 set. 2022.

SAFAT, W.; ASHGHAR, Wajiha; GILLANI, S. Andleeb. Empirical analysis for crime prediction and forecasting using machine learning and deep learning techniques. **IEEE Access**, v. 9, p. 70080–70094. 202.1Disponível em: www.doi:10.1109/ACCESS.2021.3078117. Acesso em: 26 set. 2022.

SATYA, M. Muddamsetty, *et al*. Visual explanation of black-box model: Similarity Difference and Uniqueness (SIDU) method,Pattern Recognition,Volume 127,2022, 108604,

SECRETARIA DE SEGURANÇA PÚBLICA. **Governo do Estado de São Paulo**. Disponível em: https://www.ssp.sp.gov.br/. Acesso em: 26 set. 2022.

SECURITY REPORT. Disponível em: https://www.securityreport.com.br/overview/brasil-sofreu-mais-de-885-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2021/#.Y9viYXbMK3A. Acesso em: 28 set. 2022.

SEJUSP. **Secretaria de Estado de Justiça e Segurança Pública**. Disponível em: http://www.seguranca.mg.gov.br/. Acesso em: 26 set. 2022.

SOUZA, José Renato Mendes de. **Utilização de aprendizagem de máquina na predição de crime**. Trabalho de conclusão de curso (Tecnólogo em Tecnologia em Sistemas de Computação)**,** Universidade Federal Fluminense (UFF), Rio de Janeiro, 2018.

STEC, A.; KLABJAN, D. **Forecasting crime with deep learning**. 2018. Disponível em: https://arxiv.org/abs/1806.01486. Acesso em: 13 set. 2022.

WANG, Bao *et al*. Deep learning for real-time crime forecasting and its ternarization. **Chinese Annals of Mathematics**, Series B, v. 40, n. 6, p. 949-966, 2017.