

STATE OF NEW YORK

1169

2025-2026 Regular Sessions

IN SENATE

January 8, 2025

Introduced by Sen. GONZALEZ -- read twice and ordered printed, and when printed to be committed to the Committee on Internet and Technology

AN ACT to amend the civil rights law and the executive law, in relation to the use of artificial intelligence systems

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. This act shall be known and may be cited as the "New York
2 artificial intelligence act (New York AI act)".

3 § 2. Legislative findings and intent. The legislature finds and
4 declares the following:

5 (a) A revolution in artificial intelligence (AI) has advanced to the
6 point that comprehensive regulations must be enacted to protect New
7 Yorkers.

8 (b) Artificial intelligence is already an integral part of New York-
9 ers' daily lives. In the private sector, AI is currently in use in areas
10 such as education, health care, employment, insurance, credit scoring,
11 public safety, retail, banking and financial services, media, and more
12 with little transparency or oversight. A growing body of research shows
13 that AI systems that are deployed without adequate testing, sufficient
14 oversight and robust guardrails can harm consumers and deny historically
15 disadvantaged groups the full measure of their civil rights and liber-
16 ties, thereby further entrenching inequalities. The legislature must act
17 to ensure that all uses of AI, especially those that affect important
18 life chances, are free from harmful biases, protect our privacy, and
19 work for the public good.

20 (c) Safe innovation must remain a priority for the state. New York
21 state is home to thousands of technology start-ups, many of which exper-
22 iment with new applications of AI and which have the potential to find
23 new ways to employ technology at the service of New Yorkers. The goal of
24 the legislature is to encourage safe innovation in the AI sector by
25 providing clear guidance for AI development, testing, and validation

EXPLANATION--Matter in italics (underscored) is new; matter in brackets
[-] is old law to be omitted.

LBD04409-01-5

both before a product is launched and throughout the product's life cycle.

(d) New York must establish that the burden of responsibility of proving that AI products do not cause harm to New Yorkers will be shouldered by the developers and deployers of AI. While government and civil society must act to audit and enforce human rights laws around the use of AI, the companies employing and profiting from the use of AI must lead in ensuring that their products are free from algorithmic discrimination.

(e) Close collaboration and communication between New York state and industry partners is key to ensuring that innovation can occur with safeguards to protect all New Yorkers. This legislation will ensure that lines of communication exist and that there is clear statutory authority to investigate and prosecute entities that break the law.

(f) As new forms of AI are developed beyond what is currently technologically feasible, the goal of the legislature is to use this section as a guiding light for future regulations.

(g) Lastly, it is in the interest of all New Yorkers that certain uses of AI that infringe on fundamental rights, deepen structural inequality, or that result in unequal access to services shall be banned.

§ 3. The civil rights law is amended by adding a new article 8-A to read as follows:

ARTICLE 8-A

PROTECTIONS REGARDING USE OF ARTIFICIAL INTELLIGENCE

Section 85. Definitions.

86. Unlawful discriminatory practices.

86-a. Deployer and developer obligations.

86-b. Whistleblower protections.

87. Audits.

88. High-risk AI system reporting requirements.

89. Risk management policy and program.

89-a. Social scoring AI systems prohibited.

89-b. Enforcement.

§ 85. Definitions. The following terms shall have the following meanings:

1. "Algorithmic discrimination" means any condition in which the use of an AI system contributes to unjustified differential treatment or impacts, disfavoring people based on their actual or perceived age, race, ethnicity, creed, religion, color, national origin, citizenship or immigration status, sexual orientation, gender identity, gender expression, military status, sex, disability, predisposing genetic characteristics, familial status, marital status, pregnancy, pregnancy outcomes, disability, height, weight, reproductive health care or autonomy, status as a victim of domestic violence or other classification protected under state or federal laws. Algorithmic discrimination shall not include:

(a) a developer's or deployer's testing of their own AI system to identify, mitigate, and prevent discriminatory bias;

(b) expanding an applicant, customer, or participant pool to increase diversity or redress historical discrimination; or

(c) an act or omission by or on behalf of a private club or other establishment that is not in fact open to the public, as set forth in Title II of the federal Civil Rights Act of 1964, 42 U.S.C. section 2000a(e), as amended.

2. "Artificial intelligence system" or "AI system" means a machine-based system or combination of systems, that for explicit and implicit objectives, infers, from the input it receives, how to generate outputs

1 such as predictions, content, recommendations, or decisions that can
2 influence physical or virtual environments. Artificial intelligence
3 shall not include any software used primarily for basic computerized
4 processes, such as anti-malware, anti-virus, auto-correct functions,
5 calculators, databases, data storage, electronic communications, fire-
6 wall, internet domain registration, internet website loading, network-
7 ing, spam and robocall-filtering, spellcheck tools, spreadsheets, web
8 caching, web hosting, or any tool that relates only to internal manage-
9 ment affairs such as ordering office supplies or processing payments,
10 and that do not materially affect the rights, liberties, benefits, safe-
11 ty or welfare of any individual within the state.

12 3. "Auditor" shall refer to an independent entity including but not
13 limited to an individual, non-profit, firm, corporation, partnership,
14 cooperative, or association commissioned to perform an audit.

15 4. "Consequential decision" means a decision or judgment that has a
16 material, legal or similarly significant effect on an individual's life
17 relating to the impact of, access to, or the cost, terms, or availabili-
18 ty of, any of the following:

19 (a) Employment, workers' management, or self-employment, including,
20 but not limited to, all of the following:

21 (i) Pay or promotion;

22 (ii) Hiring or termination; and

23 (iii) Automated task allocation.

24 (b) Education and vocational training, including, but not limited to,
25 all of the following:

26 (i) Assessment or grading, including, but not limited to, detecting
27 student cheating or plagiarism;

28 (ii) Accreditation;

29 (iii) Certification;

30 (iv) Admissions; and

31 (v) Financial aid or scholarships.

32 (c) Housing or lodging, including rental or short-term housing or
33 lodging.

34 (d) Essential utilities, including electricity, heat, water, internet
35 or telecommunications access, or transportation.

36 (e) Family planning, including adoption services or reproductive
37 services, as well as assessments related to child protective services.

38 (f) Health care or health insurance, including mental health care,
39 dental, or vision.

40 (g) Financial services, including a financial service provided by a
41 mortgage company, mortgage broker, or creditor.

42 (h) Law enforcement activities, including the allocation of law
43 enforcement personnel or assets, the enforcement of laws, maintaining
44 public order, or managing public safety.

45 (i) Government services.

46 (j) Legal services.

47 5. "Deployer" means a person, partnership, association or corporation
48 that uses an AI system or commerce in the state of New York or provides
49 an AI system for use by the general public in the state of New York. A
50 developer may also be considered a deployer if its actions satisfy this
51 definition.

52 6. "Deployer-employer" means a deployer that is an employer.

53 7. "Developer" means a person, partnership, or corporation that
54 designs, codes, or produces an AI system, or creates a substantial
55 change with respect to an AI system, whether for its own use in the
56 state of New York or for use by a third party in the state of New York.

1 8. "Developer-employer" means a developer that is an employer.

2 9. "Employee" means an individual who performs services for and under
3 the control and direction of an employer for wages or other remunera-
4 tion, including former employees, or natural persons employed as inde-
5 pendent contractors to carry out work in furtherance of an employer's
6 business enterprise who are not themselves employers.

7 10. "Employer" means any person, firm, partnership, institution,
8 corporation, or association that employs one or more employees.

9 11. "End user" means any individual or group of individuals that:

10 (a) is the subject of a consequential decision made entirely by or
11 with the assistance of an AI system; or

12 (b) interacts, directly or indirectly, with the relevant AI system on
13 behalf of an individual or group that is the subject of a consequential
14 decision made entirely by or with the assistance of an AI system.

15 12. "High-risk AI system" means any AI system that, when deployed:

16 (a) is a substantial factor in making a consequential decision; or (b)
17 will have a material impact on the statutory or constitutional rights,
18 civil liberties, safety, or welfare of an individual in the state.

19 13. "Software stack" means the group of individual software components
20 that work together to support the execution of an AI system.

21 14. "Substantial change" means any (a) deliberate modification to an
22 AI system that would result in material inaccuracies in the reports
23 created under section eighty-eight of this article; or (b) unintentional
24 and substantial change in the data that the AI system uses as input
25 data.

26 15. "Substantial factor" means a factor that assists in making a
27 consequential decision or is capable of altering the outcome of a conse-
28 quential decision. "Substantial factor" includes, but is not limited to,
29 any use of an AI system to generate any content, decision, prediction,
30 or recommendation that is used as a basis, in whole or in part, to make
31 a consequential decision regarding an end user.

32 § 86. Unlawful discriminatory practices. It shall be an unlawful
33 discriminatory practice:

34 1. for a developer or deployer to use, sell, or share a high-risk AI
35 system or a product featuring a high-risk AI system that produces algo-
36 rithmic discrimination; or

37 2. for a developer to use, sell, or share a high-risk AI system or a
38 product featuring a high-risk AI system that has not passed an independ-
39 ent audit, in accordance with section eighty-seven of this article, that
40 has found that the product does not in fact produce algorithmic discrim-
41 ination.

42 § 86-a. Deployer and developer obligations. 1. (a) Any deployer that
43 employs a high-risk AI system for a consequential decision must inform
44 the end user at least five business days prior to the use of such system
45 for the making of a consequential decision in clear, conspicuous, and
46 consumer-friendly terms, made available in each of the languages in
47 which the company offers its end services, that AI systems will be used
48 to make a decision or to assist in making a decision. The deployer must
49 allow sufficient time and opportunity in a clear, conspicuous, and
50 consumer-friendly manner for the consumer to opt-out of the automated
51 process and for the decision to be made by a human representative. A
52 consumer may not be punished or face any other adverse action for opting
53 out of a decision by an AI system and the deployer must render a deci-
54 sion to the consumer within forty-five days.

55 (b) If a deployer employs a high-risk AI system for a consequential
56 decision to determine whether to or on what terms to confer a benefit on

1 an end user, the deployer shall offer the end user the option to waive
2 their right to advance notice of five business days under this subdivi-
3 sion.

4 (c) If the end user clearly and affirmatively waives their right to
5 five business days' notice, the deployer shall then inform the end user
6 at least one business day before the making of the consequential deci-
7 sion in clear, conspicuous, and consumer-friendly terms, made available
8 in each of the languages in which the company offers its end
9 services, that AI systems will be used to make a decision or to assist
10 in making a decision. The deployer must allow sufficient time
11 and opportunity in a clear, conspicuous, and consumer-friendly manner
12 for the consumer to opt-out of the automated process and for the
13 decision to be made by a human representative. A consumer may not be
14 punished or face any other adverse action for opting out of a deci-
15 sion by an AI system and the deployer must render a decision to the
16 consumer within forty-five days.

17 2. Any deployer that employs a high-risk AI system for a consequential
18 decision must inform the end user within five days in a clear, conspicu-
19 ous, and consumer-friendly manner if a consequential decision has been
20 made entirely by or with assistance of an automated system. The deploy-
21 er must then provide and explain a process for the end user to appeal
22 the decision, which must at minimum allow the end user to (a) formally
23 contest the decision, (b) provide information to support their position,
24 and (c) obtain meaningful human review of the decision. A deployer must
25 respond to an end user's appeal within forty-five days of receipt of the
26 appeal. That period may be extended once by forty-five additional days
27 where reasonably necessary, taking into account the complexity and
28 number of appeals. The deployer must inform the end user of any such
29 extension within forty-five days of receipt of the appeal, together with
30 the reasons for the delay.

31 3. The deployer or developer of a high-risk AI system is legally
32 responsible for quality and accuracy of all consequential decisions
33 made, including any bias, algorithmic discrimination, and/or misinfor-
34 mation resulting from the operation of the AI system.

35 4. The rights and obligations under this section may not be waived by
36 any person, partnership, association or corporation.

37 § 86-b. Whistleblower protections. 1. Developer-employers and/or
38 deployer-employers of high-risk AI systems shall not:

39 (a) prevent an employee from disclosing information to the attorney
40 general, including through terms and conditions of employment or seeking
41 to enforce terms and conditions of employment, if the employee has
42 reasonable cause to believe the information indicates a violation of
43 this article; or

44 (b) retaliate against an employee for disclosing information to the
45 attorney general pursuant to this section.

46 2. An employee harmed by a violation of this article may petition a
47 court for appropriate relief as provided in subdivision five of section
48 seven hundred forty of the labor law.

49 3. Developer-employers and deployer-employers of high-risk AI systems
50 shall provide a clear notice to all employees working on such AI systems
51 of their rights and responsibilities under this article, including the
52 right of employees of contractors and subcontractors to use the develop-
53 er's internal process for making protected disclosures pursuant to
54 subdivision four of this section. A developer-employer or deployer-em-
55 ployer is presumed to be in compliance with the requirements of this

1 subdivision if the developer-employer or deployer-employer does either
2 of the following:

3 (a) at all times post and display within all workplaces maintained by
4 the developer-employer or deployer-employer a notice to all employees of
5 their rights and responsibilities under this article, ensure that all
6 new employees receive equivalent notice, and ensure that employees who
7 work remotely periodically receive an equivalent notice; or

8 (b) no less frequently than once every year, provides written notice
9 to all employees of their rights and responsibilities under this article
10 and ensures that the notice is received and acknowledged by all of those
11 employees.

12 4. Each developer-employer and deployer-employer shall provide a
13 reasonable internal process through which an employee may anonymously
14 disclose information to the developer if the employee believes in good
15 faith that the information indicates that the developer has violated any
16 provision of this article or any other law, or has made false or mate-
17 rially misleading statements related to its safety and security proto-
18 col, or failed to disclose known risks to employees, including, at a
19 minimum, a monthly update to the person who made the disclosure regard-
20 ing the status of the developer's investigation of the disclosure and
21 the actions taken by the developer in response to the disclosure.

22 5. This section does not limit protections provided to employees under
23 section seven hundred forty of the labor law.

24 § 87. Audits. 1. Prior to deployment of a high-risk AI system, six
25 months after deployment, and at least every eighteen months thereafter
26 for each calendar year a high-risk AI system is in use after the first
27 post-deployment audit, every developer or deployer of a high-risk AI
28 system shall cause to be conducted at least one third-party audit in
29 compliance with the provisions of this section to ensure that the prod-
30 uct does not produce algorithmic discrimination and complies with the
31 provisions of this article. Regardless of final findings, the deployer
32 or developer shall deliver all audits conducted under this section to
33 the attorney general.

34 2. A deployer or developer may hire more than one auditor to fulfill
35 the requirements of this section.

36 3. The audit shall include the following:

37 (a) an analysis of data management policies including whether personal
38 or sensitive data relating to a consumer is subject to data security
39 protection standards that comply with the requirements of section eight
40 hundred ninety-nine-bb of the general business law;

41 (b) an analysis of the system accuracy and reliability according to
42 each specified use case listed in the entity's reporting document filed
43 by the developer or deployer under section eighty-eight of this article;

44 (c) disparate impacts and a determination of whether the product
45 produces algorithmic discrimination in violation of this article by each
46 intended and foreseeable identified use as identified by the deployer
47 and developer;

48 (d) analysis of how the technology complies with existing relevant
49 federal, state, and local privacy and data privacy laws; and

50 (e) an evaluation of the developer's or deployer's documented risk
51 management policy and program required under section eighty-nine of this
52 article for conformity with subdivision one of such section eighty-nine.

53 4. The attorney general may promulgate further rules as necessary to
54 ensure that audits under this section assess whether or not AI systems
55 produce algorithmic discrimination and otherwise comply with the
56 provisions of this article.

1 5. The independent auditor shall have complete and unredacted copies
2 of all reports previously filed by the deployer or developer under
3 section eighty-eight of this article.

4 6. An audit conducted under this section shall be completed in its
5 entirety without the assistance of an AI system.

6 7. (a) An auditor shall be an independent entity including but not
7 limited to an individual, non-profit, firm, corporation, partnership,
8 cooperative, or association.

9 (b) For the purposes of this article, no auditor may be commissioned
10 by a developer or deployer of an AI system if such entity has already
11 been commissioned to provide any auditing or non-auditing service,
12 including but not limited to financial auditing, cybersecurity auditing,
13 or consulting services of any type, to the commissioning company in the
14 past twelve months.

15 (c) Fees paid to auditors may not be contingent on the result of the
16 audit and the commissioning company shall not provide any incentives or
17 bonuses for a positive audit result.

18 8. The attorney general may promulgate further rules to ensure (a) the
19 independence of auditors under this section, and (b) that teams conduct-
20 ing audits incorporate feedback from communities that may foreseeably be
21 the subject of algorithmic discrimination with respect to the AI system
22 being audited.

23 § 88. High-risk AI system reporting requirements. 1. Every developer
24 and deployer of a high-risk AI system shall comply with the reporting
25 requirements of this section. Regardless of final findings, reports
26 shall be filed with the attorney general prior to deployment of a high-
27 risk AI system and then annually, or after each substantial change to
28 the system, whichever comes first.

29 2. Together with each report required to be filed under this section,
30 developers and deployers shall file with the attorney general a copy of
31 the last completed independent audit required by this article and a
32 legal attestation that the high-risk AI system: (a) does not violate
33 any provision of this article; or (b) may violate or does violate one or
34 more provisions of this article, that there is a plan of remediation to
35 bring the high-risk AI system into compliance with this article, and a
36 summary of such plan of remediation.

37 3. Developers of high-risk AI systems shall file with the attorney
38 general a report containing the following:

39 (a) a description of the system including:

40 (i) a description of the system's software stack;

41 (ii) the purpose of the system;

42 (iii) the system's use to end users; and

43 (iv) reasonably foreseeable uses outside of the current or intended
44 uses;

45 (v) how the system should be used or not used;

46 (b) the intended outputs of the system and whether the outputs can be
47 or are otherwise appropriate to be used for any purpose not previously
48 articulated;

49 (c) the methods for training of their models including:

50 (i) any pre-processing steps taken to prepare datasets for the train-
51 ing of a model underlying a high-risk AI system;

52 (ii) datasheets comprehensively describing the datasets upon which
53 models were trained and evaluated, how and why datasets were collected,
54 how that training data will be used and maintained going forward through
55 the development cycle; and

1 (iii) steps taken to ensure compliance with privacy, data privacy,
2 data security, and copyright laws;

3 (d) detailed use and data management policies;

4 (e) any other information necessary to allow the deployer to under-
5 stand the outputs and monitor the system for compliance with this arti-
6 cle;

7 (f) any other information necessary to allow the deployer to comply
8 with the requirements of subdivision four of this section; and

9 (g) for any high-risk AI system that is a substantial factor in making
10 a consequential decision:

11 (i) a detailed description of the proposed uses of the system, includ-
12 ing what consequential decisions the system will support;

13 (ii) a detailed description of the system's capabilities and any
14 developer-imposed limitations, including capabilities outside of its
15 intended use, when the system should not be used, any safeguards or
16 guardrails in place to protect against unintended, inappropriate, or
17 disallowed uses, and testing of any such safeguards or guardrails;

18 (iii) an internal risk assessment including documentation and results
19 of testing conducted to identify all reasonably foreseeable risks
20 related to algorithmic discrimination, accuracy and reliability, privacy
21 and autonomy, and safety and security, as well as actions taken to
22 address those risks, and subsequent testing to assess the efficacy of
23 actions taken to address risks; and

24 (iv) whether the system should be monitored, and if so, how such
25 system should be monitored.

26 4. Deployers of high-risk AI systems shall file with the attorney
27 general a report containing the following:

28 (a) a description of the system including:

29 (i) a description of the system's software stack;

30 (ii) the purpose of the system;

31 (iii) the system's use to end users; and

32 (iv) reasonably foreseeable uses outside of the current or intended
33 uses;

34 (b) the intended outputs of the system and whether the outputs can be
35 or are otherwise appropriate to be used for any purpose not previously
36 articulated;

37 (c) assessment of the relative benefits and costs to the consumer
38 given the system's purpose, capabilities, and probable use cases;

39 (d) whether the deployer collects revenue or plans to collect revenue
40 from use of the high-risk AI system, and if so, how it monetizes or
41 plans to monetize use of the system; and

42 (e) for any high-risk AI system that is a substantial factor in making
43 a consequential decision:

44 (i) a detailed description of the proposed uses of the system, includ-
45 ing what consequential decisions the system will support;

46 (ii) whether the system is designed to make consequential decisions
47 itself or whether and how it supports consequential decisions;

48 (iii) a detailed description of the system's capabilities and any
49 deployer-imposed limitations, including capabilities outside of its
50 intended use, when the system should not be used, any safeguards or
51 guardrails in place to protect against unintended, inappropriate, or
52 disallowed uses, and testing of any such safeguards or guardrails;

53 (iv) an assessment of the relative benefits and costs to the consumer
54 given the system's purpose, capabilities, and probable use cases;

55 (v) an internal risk assessment including documentation and results of
56 testing conducted to identify all reasonably foreseeable risks related

1 to algorithmic discrimination, accuracy and reliability, privacy and
2 autonomy, and safety and security, as well as actions taken to address
3 those risks, and subsequent testing to assess the efficacy of actions
4 taken to address risks; and

5 (vi) whether the system should be monitored, and if so, how such
6 system should be monitored.

7 5. The attorney general shall:

8 (a) promulgate rules for a process whereby developers and deployers
9 may request redaction of portions of reports required under this section
10 to ensure that they are not required to disclose sensitive and protected
11 information; and

12 (b) maintain an online database that is accessible to the general
13 public with reports, redacted in accordance with this subdivision, and
14 audits required by this article which shall be updated biannually.

15 6. For high-risk AI systems which are already in deployment at the
16 time of the effective date of this article, developers and deployers
17 shall have eighteen months from such effective date to complete and file
18 the reports and independent audit required by this article.

19 § 89. Risk management policy and program. 1. Each developer or deploy-
20 er of high-risk AI systems shall plan, document, and implement a risk
21 management policy and program to govern development or deployment, as
22 applicable, of such high-risk AI system. The risk management policy and
23 program shall specify and incorporate the principles, processes, and
24 personnel that the deployer uses to identify, document, and mitigate
25 known or reasonably foreseeable risks of algorithmic discrimination
26 covered under subdivision one of section eighty-six of this article. The
27 risk management policy and program shall be an iterative process
28 planned, implemented, and regularly and systematically reviewed and
29 updated over the life cycle of a high-risk AI system, requiring regular,
30 systematic review and updates, including updates to documentation. A
31 risk management policy and program implemented and maintained pursuant
32 to this section shall be reasonable considering:

33 (a) The guidance and standards set forth in version 1.0 of the "Arti-
34 ficial Intelligence Risk Management Framework" published by the National
35 Institute of Standards and Technology in the United States department of
36 commerce, or the latest version of the "Artificial Intelligence Risk
37 Management Framework" published by the National Institute of Standards
38 and Technology if, in the attorney general's discretion, the latest
39 version of the "Artificial Intelligence Risk Management Framework"
40 published by the National Institute of Standards and Technology in the
41 United States department of commerce is at least as stringent as version
42 1.0;

43 (b) The size and complexity of the developer or deployer;

44 (c) The nature, scope, and intended uses of the high-risk AI system
45 developed or deployed; and

46 (d) The sensitivity and volume of data processed in connection with
47 the high-risk AI system.

48 2. A risk management policy and program implemented pursuant to subdivi-
49 sion one of this section may cover multiple high-risk AI systems
50 developed by the same developer or deployed by the same deployer if
51 sufficient.

52 3. The attorney general may require a developer or a deployer to
53 disclose the risk management policy and program implemented pursuant to
54 subdivision one of this section in a form and manner prescribed by the
55 attorney general. The attorney general may evaluate the risk management
56 policy and program to ensure compliance with this section.

§ 89-a. Social scoring AI systems prohibited. No person, partnership, association or corporation shall develop, deploy, use, or sell an AI system which evaluates or classifies the trustworthiness of natural persons over a certain period of time based on their social behavior or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

1. differential treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; or

2. differential treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behavior or its gravity.

§ 89-b. Enforcement. 1. Whenever there shall be a violation of any provision of this article, an application may be made by the attorney general in the name of the people of the state of New York, to the supreme court having jurisdiction by a special proceeding to issue an injunction, and upon notice to the respondent of not less than ten days, to enjoin and restrain the continuance of such violation; and if it shall appear to the satisfaction of the court that the respondent has, in fact, violated this article, an injunction may be issued by the court, enjoining and restraining any further violations, without requiring proof that any person has, in fact, been injured or damaged thereby. In any such proceeding, the court may make allowances to the attorney general as provided in paragraph six of subdivision (a) of section eighty-three hundred three of the civil practice law and rules, and direct restitution. Whenever the court shall determine that a violation of this article has occurred, the court may impose a civil penalty of not more than twenty thousand dollars for each violation.

2. There shall be a private right of action by plenary proceeding for any person harmed by any violation of this article by any natural person or entity. The court shall award compensatory damages and legal fees to the prevailing party.

3. In evaluating any motion to dismiss a plenary proceeding commenced pursuant to subdivision two of this section, the court shall presume the specified AI system was created and/or operated in violation of a specified law or laws and that such violation caused the harm or harms alleged.

(a) A defendant can rebut presumptions made pursuant to this subdivision through clear and convincing evidence that the specified AI system did not cause the harm or harms alleged and/or did not violate the alleged law or laws. An algorithmic audit can be considered as evidence in rebutting such presumptions, but the mere existence of such an audit, without additional evidence, shall not be considered clear and convincing evidence.

(b) Where such presumptions are not rebutted pursuant to this subdivision, the action shall not be dismissed.

(c) Where such presumptions are rebutted pursuant to this subdivision, a motion to dismiss an action shall be adjudicated without any consideration of this section.

4. The supreme court in the state shall have jurisdiction over any action, claim, or lawsuit to enforce the provisions of this article.

§ 4. Section 296 of the executive law is amended by adding a new subdivision 23 to read as follows:

23. It shall be an unlawful discriminatory practice under this section for a deployer or a developer, as such terms are defined in section

- 1 eighty-five of the civil rights law, to engage in an unlawful discrimi-
2 natory practice under section eighty-six of the civil rights law.
3 § 5. This act shall take effect immediately.