With the increasing threats of computer hackers and the damages they are able to (and have) caused, it is no wonder that there is now a great deal of laws to define what is legal and what is not legal behavior on a computer or computer network. Analyzing these laws provides a general idea of what is right and wrong in cyberspace. The intention of most state and federal laws is to prohibit unauthorized use of computers and computer networks and to prohibit intercepting data sent from one computer to another while most Internet Service Providers (in our case, the Georgia Institute of Technology is our provider) go a little bit farther to define what is acceptable use of the computers and the networks that they service.

There are several federal laws that define unauthorized computer use and the penalties associated with such use. Under Title 18 of the U.S. Code, Sections 1030, 2511, and 2701 all apply to computer and computer network use. In particular, Section 1030 prohibits unauthorized use of government and financial computer systems and other uses that might harm national security. It also prohibits the transmission of any kind of program or code that is intended to damage a computer. It also specifically makes password stealing and sharing illegal. Section 2511 prohibits the interception of electronic communications (such as data on networks) and Section 2701 prohibits viewing, altering, or removing data stored on some type of electronic storage. These sections carry various punishments that include some type of fine (the actual amount appears to be undefined) and from 1 to 20 years of imprisonment depending on the nature of the offense (fraud, under Section 1030, appears to carry heavier sentences). These federal laws do not appear to make port scanning a crime.
Because the above federal laws are somewhat limited in their jurisdiction (some laws only apply to attacks on government or financial computer systems and networks), Georgia has its own laws to contend with computer hacking. The foremost of these is the Georgia Computer Systems Protection Act. This law makes it illegal to delete or remove data or programs without authorization as well as making it illegal to interfere or obstruct with the normal use of a program or of data. It also makes it illegal to examine medical records, salaries, or other financial or personal data without authorization. Finally, it prohibits disclosing passwords (password trafficking). The Georgia law states that the criminal penalties for these violations result in a fine of no more than $50,000 or imprisonment of less than 15 years. Trafficking in passwords results in no more than a $5,000 fine or imprisonment of up to one year. The Georgia law also specifically allows for damages to be sought in a civil court (i.e. the perpetrator can be sued). The Georgia law also does not appear to make port scanning a crime.

The Georgia Institute of Technology Office of Information Technology provides a “Network Usage Policy” to govern the use of computers and computer networks at Georgia Tech. Whereas most of this policy is designed to reiterate the above laws, it further restricts network usage in two major areas. First, the policy prohibits the use of encryption programs without prior approval (section 3.1.1). Second, it also specifically prohibits port scanning (section 4.6.3). If a user is found in violation of this policy and the violation is deemed a “minor” violation, that user will first be issued a warning. Following that warning (or in the case of a “major” violation), the user will be turned over to Student Affairs (for students) or to the Unit Head (for employees) for disciplinary action. If the violation is also a violation of a state or federal law, than the user may be reported to the appropriate authorities.

One can conclude from these laws that, in general, using a computer or computer network
without authorization is indeed a criminal offense. Port scanning other computers appears to not be in violation of a state or federal law unless it causes the malfunction of a computer (some network devices have been known to experience a denial-of-service when port scanned).

However, port scanning is explicitly denied when it involves systems at the Georgia Institute of Technology. While the federal and state laws provide most of the legal framework for legal and illegal computer usage, Georgia Tech goes a step farther to explicitly prohibit certain usages of their computers and networks.

Georgia Computer Systems Protection Act

Georgia Institute of Technology - Office of Information Technology - Network Usage Policy
[http://www.security.gatech.edu/policy/usage/policy.html](http://www.security.gatech.edu/policy/usage/policy.html)

Federal Laws - Title 18 Sections 1030, 2511, 2701
[http://www4.law.cornell.edu/uscode/18/1030.html](http://www4.law.cornell.edu/uscode/18/1030.html)
[http://www4.law.cornell.edu/uscode/18/2511.html](http://www4.law.cornell.edu/uscode/18/2511.html)
[http://www4.law.cornell.edu/uscode/18/2701.html](http://www4.law.cornell.edu/uscode/18/2701.html)